KPMG Consulting

JUSTIS
Justice Information System For the District of Columbia
Blueprint

January 15, 2001

Delivered to the Criminal Justice Coordinating Council & The Office of the Chief Technology Officer

In conjunction with

Contract Number: GS-35F-4338D
Delivery Order: #AT0P0002360

DISTRICT OF COLUMBIA GOVERNMENT

CRIMINAL JUSTICE COORDINATING COUNCIL

JUSTIS SYSTEM BLUEPRINT

January 15, 2001

~ Table of Contents ~

~ Figures ~

1. Introduction

1.1 Background

The Criminal Justice Coordinating Council of the District of Columbia (CJCC) was organized with the following mission:

> To serve as the forum for identifying issues and their solutions, proposing actions, and facilitating cooperation that will improve public safety and the related criminal and juvenile justice services for District of Columbia residents, visitors, victims, and offenders. The CJCC draws upon local and federal agencies and individuals to develop recommendations and strategies for accomplishing this mission. Our guiding principles are creative collaboration, community involvement, and effective resource utilization. We are committed to developing targeted funding strategies and comprehensive management information through integrated information technology systems and social science research in order to achieve our goal.[1]

In 1999 the CJCC of the District of Columbia, supported by its Policy and Budget Working Group (P&BWG), produced a federal funding strategy, recommended a governance structure, and prepared an *Information Technology Interagency Agreement* that the CJCC members adopted. This agreement recognized the need for immediate improvement of information technology in the criminal justice system within the District of Columbia and established the Information Technology Advisory Committee (ITAC) to serve as the governance body for justice system development.

The ITAC has been given the duty of advising and making recommendations to the CJCC in regards to improvement of the information technology infrastructure of justice agencies within the District of Columbia. The recommendations are to be made in respect to increased funding of information technology projects, increased data sharing, access, and integration, improved data and system security, and the development of system-wide standards and measurement of data use and quality, as appropriate to the then-current developmental stage of the justice system. The recommendations by the ITAC are developed based on the following guiding principles:[2]

- Recognize the primacy of each justice agency mission
- Facilitate collaborative solutions to justice information challenges
- Commit to the quality and integrity of justice data
- Implement effective data and system security
- Respect the confidentiality of information and individual privacy
- Establishment of system-wide standards, supported by common identifiers and positive identification
- Nurture agency and community requirements for research and public access

[1] http://www.cjccdc.org
[2] *Ibid.*

- Provide for long-term performance monitoring and evaluation

Recognizing that the information systems currently maintained by the justice agencies within the District are difficult to access, the ITAC envisioned a system that would promote the sharing of justice data while maintaining the primacy of each justice agency. The solution is a District of Columbia Justice Information System (JUSTIS).

In July 2000, the CJCC partnered with the Office of the Chief Technology Officer (OCTO) in contracting KPMG Consulting, LLC (KPMG) to design a solution concept that is based on modern dedicated Intranet and web browser technologies that support secure, confidential data access, data sharing, and notification functionality. It is imperative that the solution concept is designed not to disrupt the existing legacy systems of the individual agencies or demand costly and inefficient data collection and transfer. The design is to be delivered to the ITAC in the form of a JUSTIS Blueprint. The first phase of JUSTIS System development is to take the form of a functioning proof-of-concept.

1.2 Implementation Strategy

This document is the JUSTIS Blueprint for the implementation of the JUSTIS System and is to establish lay the foundation for CJCC's envisioned solution. The JUSTIS Blueprint is a vision of the ultimate system, an analysis of current state capabilities and requirements, and a definition of steps to take for a multi-phased implementation. This Blueprint is also to provide a high-level architecture and roadmap for the development of the JUSTIS System.

The JUSTIS System Blueprint is developed with the intention of a multi-phased approach. A multi-phased implementation is designed to provide enhanced JUSTIS System functionalities to be implemented with phases in a three- to six-month time frame. Such an implementation provides several advantages over a large, full-scale implementation. A phased implementation:

- Provides short-term successes
- Allows time for validation of the long-term plan after each phase
- Allows for the integration of current technologies throughout the implementation

A representative diagram of a possible JUSTIS System multi-phased implementation follows:

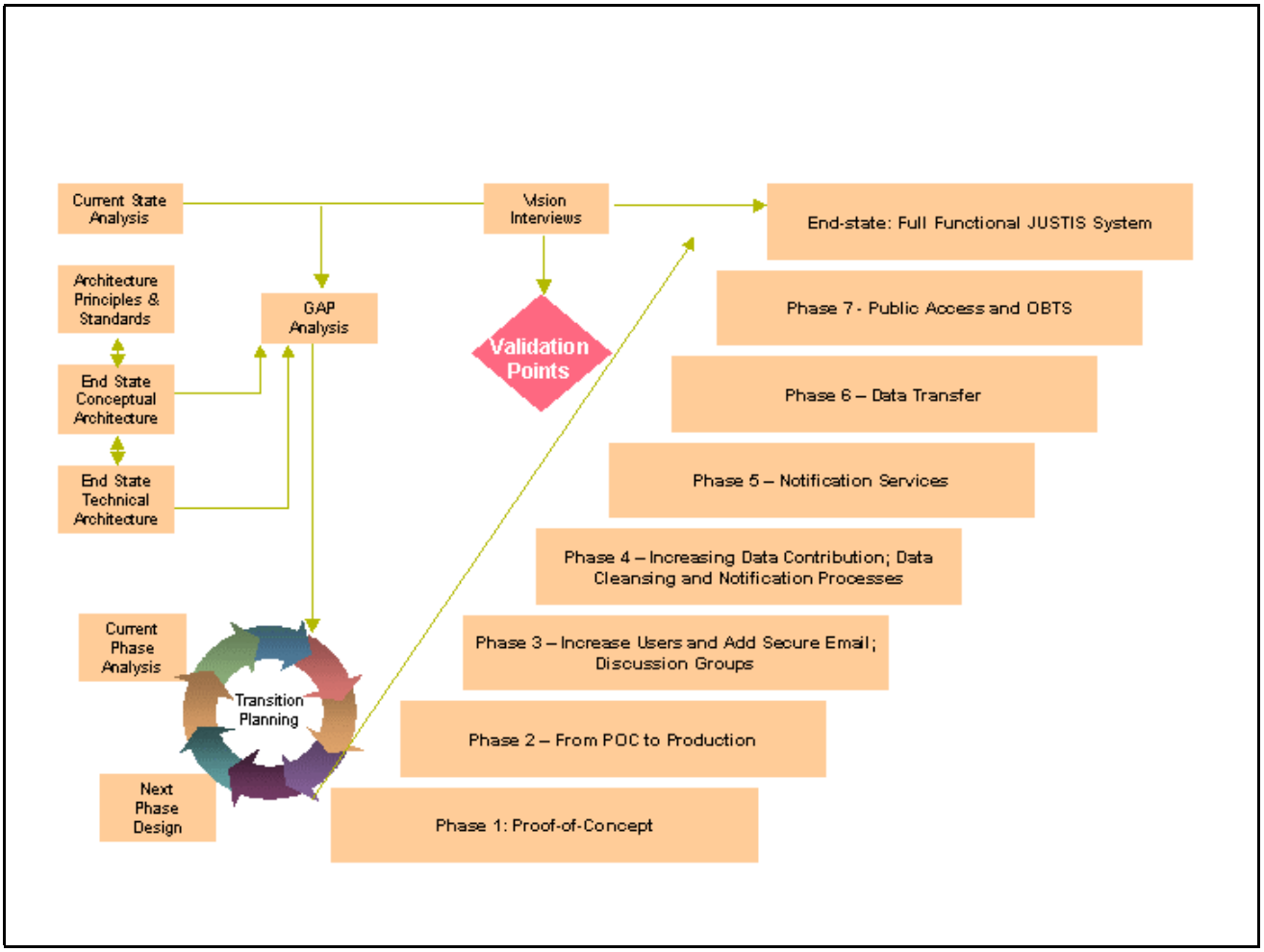


Figure 1 – Representative JUSTIS Phased Implementation

The beginning of a multi-phase implementation as represented in Figure 1 is an analysis of the current state of the justice agencies' business processes and information technology infrastructure. Coinciding with this analysis is the coordinating of key justice agency personnel's foresight in the form of "Vision Interviews." System validation points are developed from the vision interviews.

The full functional JUSTIS System is considered "End State" in the figure. The JUSTIS System design is derived from a foundation of agreed upon architecture principles and standards. The JUSTIS System architecture is refined by the agreed upon principles and standards. The technical architecture of the system is generated from the conceptual architecture. This evolution of the design of the JUSTIS System creates the End State solution.

Transition planning, is the integration of the current state analysis and the end state solution that generates a list of "gap" points. The gap points are logically prioritized according to both business and technological constraints and the aforementioned vision interviews. The prioritization of gap points develops the multi-phased implementation. Throughout the multi-phased implementation, each phase must be validated against the original vision of the JUSTIS System to ensure the implementation remains true to that vision.

The JUSTIS System multi-phased implementation has begun with the development and deployment of a working proof-of-concept (POC). The POC uses the same open Internet technologies and standards to link information from diverse justice agency systems as will be designed in the JUSTIS System Architecture. The POC gives the CJCC and the selected pilot agencies an early look at the JUSTIS architecture and functionality. Also, the selected authorized users can share certain information and observe the on-going development of the JUSTIS System.

1.3 Blueprint Format

The Blueprint defines and recommends the necessary elements for the CJCC to implement the JUSTIS System. The Blueprint accomplishes this in the following manner:

1. **Defining the Future JUSTIS System.** It is important to define the ideal future system first, without concern for the current capabilities. This ensures maximum creativity on the part of the participants. KPMG conducted numerous vision interviews with key CJCC members during the months of July and August 2000. We also considered capabilities in the KPMG JNET solution developed for the Commonwealth of Pennsylvania.

2. **Defining the current technical infrastructure in the justice agencies in the District of Columbia.** The first step defined where we want to end up with our JUSTIS System. This step shows the point from which we will begin.

3. **Conducting a Gap Analysis.** In this step, we show the distance that needs to be closed in moving from the current state towards the target end state.

4. **Recommending the Roadmap that will bring the Future JUSTIS System to reality in the justice agencies within the District of Columbia.** This roadmap recognizes the importance of a phased implementation, as discussed above.

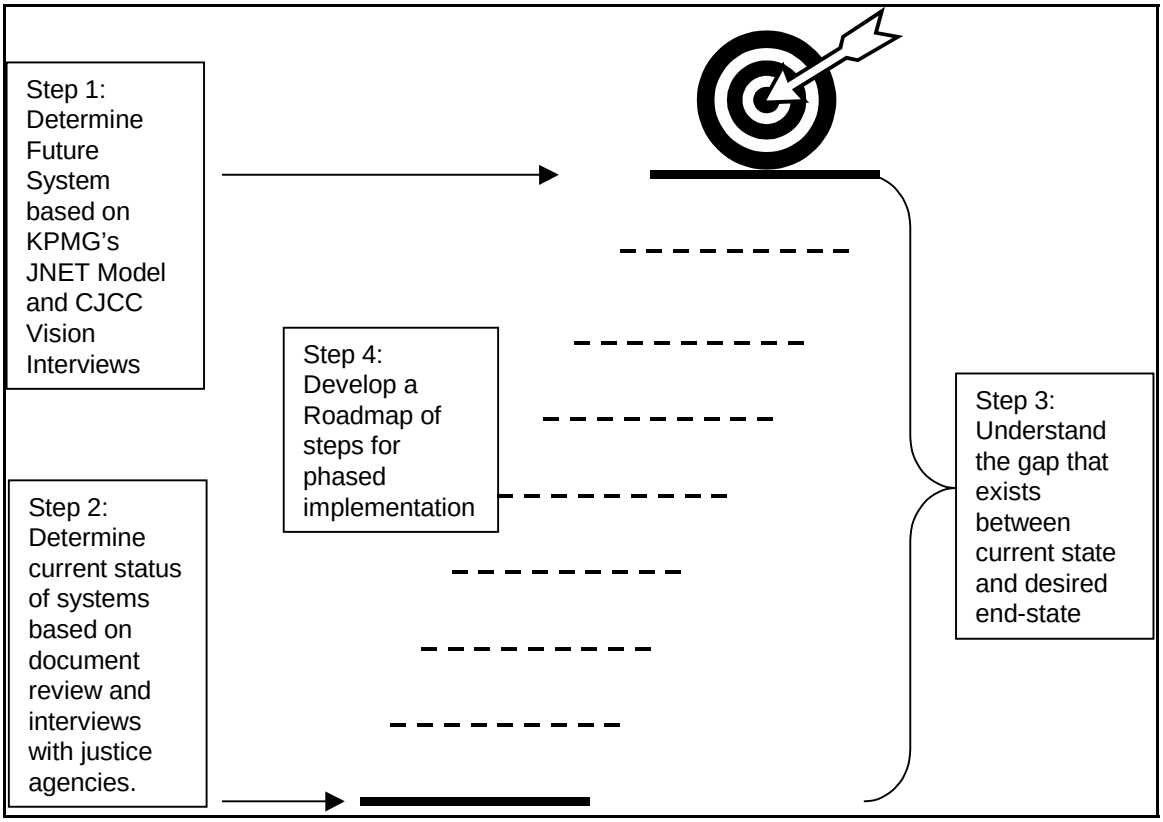


Figure 2 – Blueprint Format

2. JUSTIS System Business Requirements and Goals

2.1 JUSTIS System Business Requirements

The CJCC has taken the initiative in pursuing and managing necessary business requirements within the justice community of the District of Columbia that will lead to the accomplishment of its stated objectives. These business requirements are continually referenced throughout the development of the JUSTIS System.

- **Implement industry best practices for information security.** The JUSTIS System requires system-wide security policies. The CJCC has taken the initiative to develop security policies that meet or exceed the security requirements of the member agencies and draws upon elements from the NCIC standards.

- **Encourage the use of a common District-wide identifier.** The data shared in the JUSTIS System can be designed to be retrievable by a common District-wide identifier, such as the PDID or the Arrest Number. Having a common identifier will enable many of the functions of JUSTIS and will assist justice agencies within the District in coordinating their information processing.

- **Foster interagency participation and collaboration.** The JUSTIS System enables participation of all District and Federal justice agencies. The JUSTIS System's ease of use creates an environment that promotes interagency participation and collaboration.

- **Streamline processing that crosses agency boundaries.** The streamlining of agency processes increases efficiency and effectiveness. The implementation of the JUSTIS System integrates technology into currently manual process. The reduction of manual processes will streamline processes across agency boundaries.

- **Recognize the independence and primacy of each justice agency**. Although agency coordination and consensus is a necessary business requirement, effective agency governance and representation is just as critical. The JUSTIS System recognizes agency primacy and is designed to be considerate of individual agency decision-making.

- **Employ open technologies.** The use of open technologies also contributes to the independence of individual agencies. Agencies can make changes to other information systems with minimum impact on the JUSTIS System.

The CJCC is committed to making the many justice agencies within the District of Columbia function in unison with information sharing as a backbone. The District of Columbia's JUSTIS System is designed to provide a platform for this information sharing through the use of "connections." The JUSTIS System provides connections between people and information (information inquiry applications and search engines); connections between people and people (newsgroups, secure email) and connections between information and information (e.g., data transfer, data scrubbing notification). The JUSTIS System is designed to contribute to the objectives of the CJCC.

2.2 JUSTIS System Goals

In addition to the business requirements imposed on JUSTIS, there are a number of fundamental goals for the system: collaboration, information sharing, effective resource utilization and information management.

2.2.1 Collaboration

The JUSTIS System enables collaborative solutions to justice information challenges. Agencies can work together in case management and transition. For example, an offender contact list can be published through the JUSTIS System. This offender contact list will provide the contact information for case handlers, such as the attorneys assigned to the case, the judge assigned, the arresting law enforcement official, and any other individuals within the justice agencies that could be of importance. The list would provide one area to obtain key contacts for an individual offender.

Another opportunity for collaboration is through the use of discussion groups. Authorized users could participate in on-line discussions regarding justice issues, case management, and the like.

Notification applications outlined in the JUSTIS System provide yet another opportunity for justice agency collaboration. The notification could be on an individual basis or a group basis. For example, when a parolee is arrested and booked, this event (the police booking) can generate a notification to an individual parole officer or group of interested parties.

2.2.2 Information Sharing

Interagency sharing of data supports each agency's ability to make quality decisions. The JUSTIS System provides a platform for the sharing of critical justice information on a timely basis and in a secure environment. This allows justice agencies to share selected information that will assist each justice agency in conducting its mission-critical activities.

The CJCC's decision to take advantage of modern dedicated Intranet and web browser technologies allows for the publishing of data in a timely fashion. One example of an information sharing opportunity that can be enhanced with the implementation of the JUSTIS System is changes in case disposition. Any change in a case disposition made by any justice agency can be "published" (translated to a standard web-accessible format and forwarded) using the JUSTIS System**.** Any authorized JUSTIS user could then locate and retrieve the current case disposition of an offender.

2.2.3 Effective Resource Utilization

Currently, interagency data exchanges are either not taking place or are performed using inefficient manual processes. The JUSTIS System allows resources to use information system solutions to become more effective contributors and reduce labor-intensive information searches. For example, many justice agencies are in need of the daily "lock-up list" produced by the Metropolitan Police Department (MPD). The acquisition of this list in a timely manner by each agency requires labor-intensive processes. The implementation of the JUSTIS System could allow the lock-up list to be published as soon as it is produced by MPD, therefore eliminating any need for other agencies to commit resources in the acquiring of this list.

The JUSTIS System also allows for the opportunity of data transfer. The concept allows for common data to be identified and captured through the browser. The authorized user could then potentially copy the data and use it to populate a corresponding common data field in the agency's legacy system. This eliminates the redundant activity of re-keying common information from system to system**.** This also reduces potential errors caused by keying mistakes when transferring data from system to system.

2.2.4 Information Management

Information systems for the justice community must implement effective data and system security. The JUSTIS System provides for indirect data retrieval. This allows for a significant decrease in security risk to the legacy systems and absolutely no risk of data corruption. Authorized users will enter the JUSTIS System and view published data that has been obtained either through direct access through a firewall to the legacy system, indirect access through a firewall to an intermediary server, or off-line access, where the data is loaded into the JUSTIS System through some other media. Thus the inquiry will not have direct unsecured access to the legacy system.

Additionally, a tenet of JUSTIS System is to not interfere with, compete with, or replace current legacy systems. The JUSTIS System is not a data warehouse. Therefore there is no central repository of data and the data stay within the agency's IT infrastructure.

3. Future JUSTIS User Community and System

3.1 Introduction

The JUSTIS System supports the justice community and each of its member agencies. This section describes the fully functional system, the model that comprises the overall solution, the proposed user community, the technical architecture, and the organizational structure necessary to manage and administer the system.

This section concentrates on describing the future "to be" JUSTIS System. Subsequent sections will address the current state and strategies for getting from where we are to where we want to be. Because this is a Blueprint document, it seems appropriate to use the following building metaphor to organize this section:

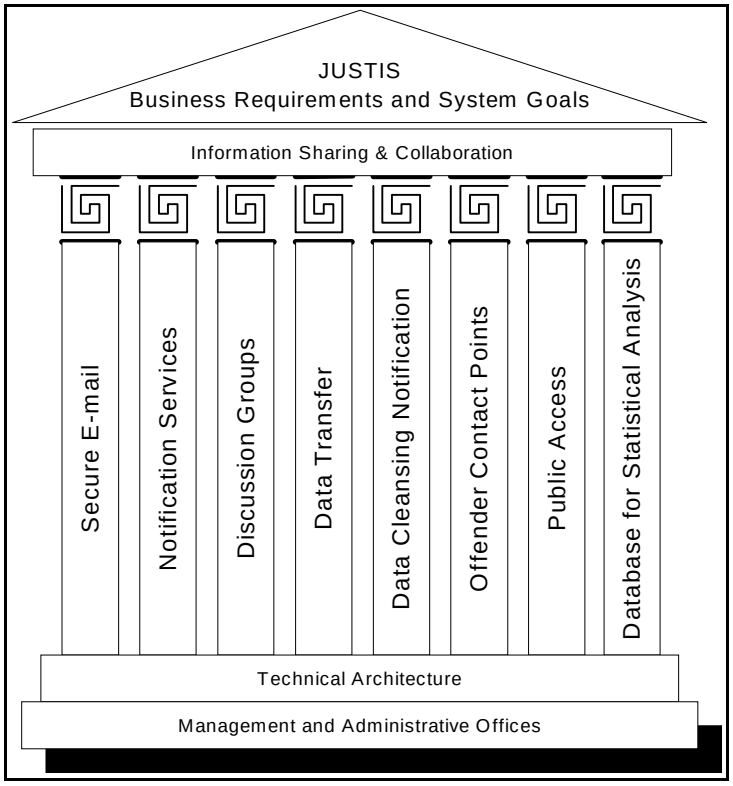


Figure 3 – Blueprint Building Metaphor

In this section, we will start from the top of the diagram and proceed toward the bottom. We have already discussed the business requirements and system goals that JUSTIS is designed to meet. In this section, we will:

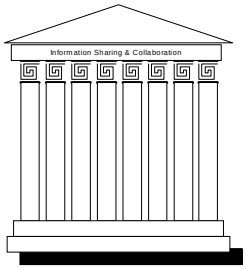
- Discuss the functional components that empower JUSTIS and its users to achieve the business requirements and system goals. "Information Sharing and Collaboration" is shown across the top of our diagram because it is the very essence – the capstone – of the system. (See section 3.2 Agency Information Sharing)

- Discuss the supporting functional components. Shown as columns in the diagram, these functions of JUSTIS support information sharing and collaboration. (See section 3.3 Interagency Functions Supported by the JUSTIS System)

- Discuss the technical architecture that is needed to support the functional components. The functional discussion has shown *what* the system will do. The technical architecture section will show *how* the system will do it. (See section 3.4 Technical Architecture)

- Finally, the management and administrative office structure necessary to support the JUSTIS System is described. Shown at the bottom of our diagram, this organization will be the bedrock and foundation for JUSTIS. (See section 3.5 Management and Administrative Structure)

3.2 Agency Information Sharing and Collaboration



The JUSTIS System is designed to provide justice agencies a quick and effective way to share justice information and collaborate with colleagues. The value provided by JUSTIS to the user community is in direct relation to the number of participating agencies – both contributors and consumers.

The JUSTIS System will enable its users to share justice information through a variety of modes:

- **JUSTIS Query Applications** – Record queries allow individual JUSTIS agencies to access the data in other agencies' systems. Predefined queries allow information to become dynamic. The authorized user accesses the queries, fills the required information and submits. The system returns a unified view of queried information. Note that queries submitted, logins and other user activity are recorded to an audit log.

- **Searches** – Information sharing is improved beyond predetermined queries when information searches are enabled. These searches can be conducted across the entire World Wide Web or within the JUSTIS framework of static pages and other content.

- **Static Screens and Printed Reports** – Agencies will be able to share information through the publishing of static screens. Static screens display content in Hypertext Markup Language (HTML) and are delivered to a web browser using Hypertext Transfer Protocol (HTTP). This information is not dynamic, therefore it cannot be changed due to user input. The ability to publish agency reports on the web is an efficient form of information dissemination. Agency reports can be published in HTML as well as PDF formats using the appropriate "plug-in" software. Authorized users can download these published reports.

- **Threaded Discussion Groups** – Discussion groups further enhance information sharing by allowing inter-agency interaction. Discussion groups allow authorized users to post messages for response by other authorized users or data administrator.

- **Secure Email** – Secure email allows direct interaction between authorized users. Through the implementation of required security email software, secure email is enabled.

- **Notification Services** – Notification services enables data to interact with authorized users. This level of information sharing goes beyond the others and allows certain changes in data to notify specified users.

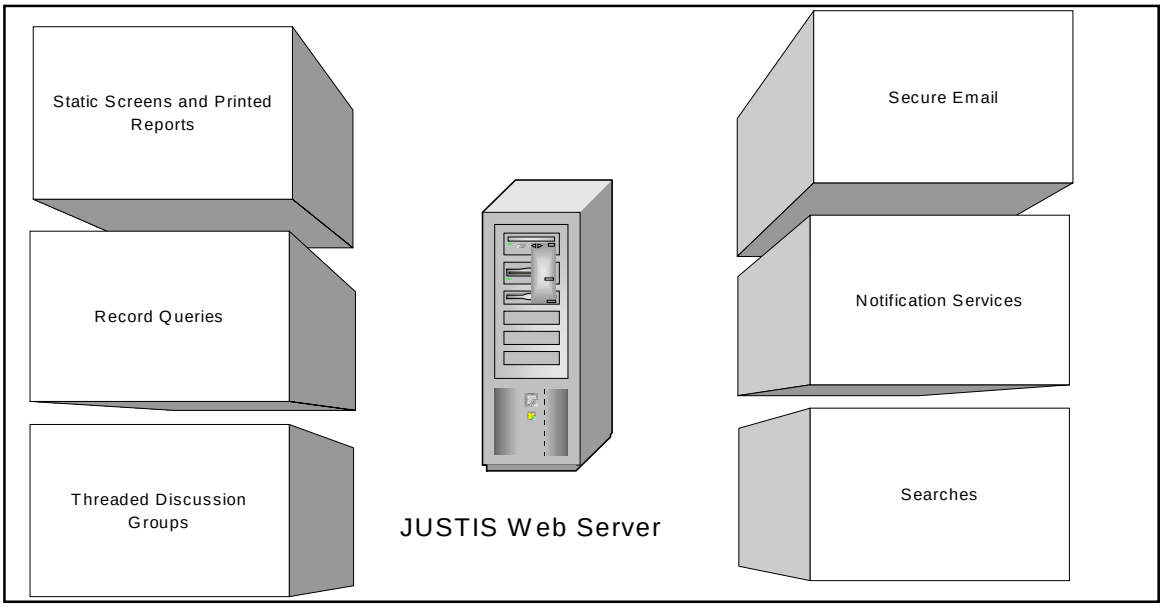


Figure 4 – JUSTIS System Information Sharing Modes

Information sharing will be obtained through the use of a secure justice system-wide Intranet. Through the JUSTIS System, community agencies will each be able to have a unified view of justice information. This unified view is currently not possible because each agency's legacy system holds an individual island of information. JUSTIS connects these islands into a unified system available to answer user queries. This section details the data each agency has chosen to share.

Subsequent sections will provide details on the modes of searches, static screens and printed reports, threaded discussion groups, secure email and notification services. The remainder of this section provides details on the JUSTS query applications (referred to as Criminal Justice Inquiry or CJI).

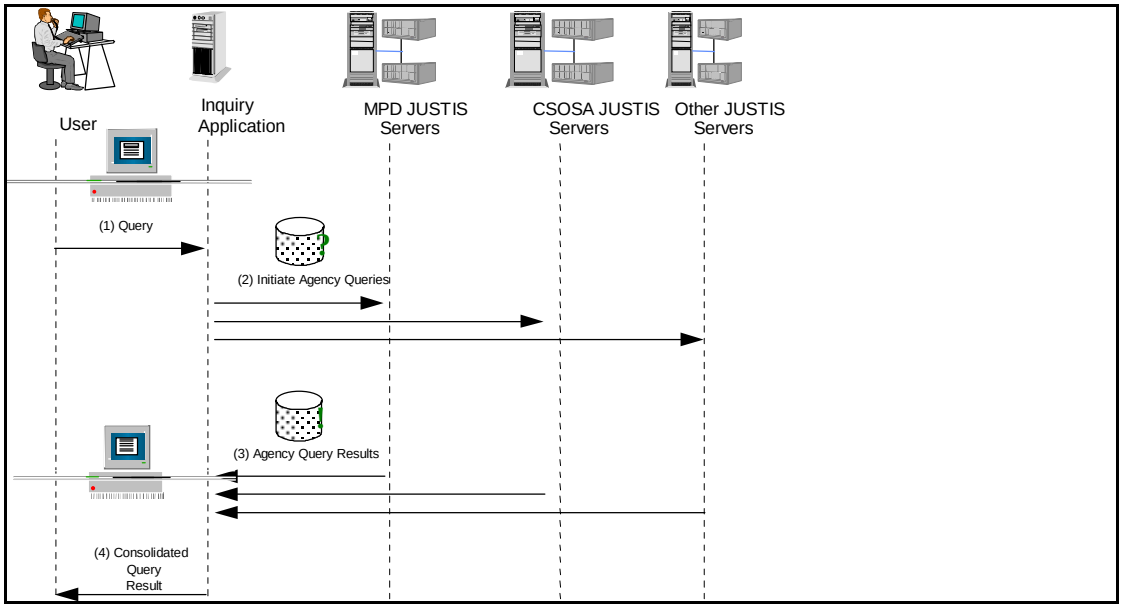


Figure 5 – Criminal JUSTIS Inquiry Application Flow

The Criminal Justice Inquiry will provide a criminal justice worker with data from criminal justice agency sources via a single-point search application and user interface. Typically, the data sources will reside in databases controlled by individual agencies.

Search results are organized in a file and folder metaphor. The architecture of this application must allow for the ability to incorporate new types (documents) and new sources (agencies) of information as they come on line, without having to be rewritten or requiring extensive re-configuration. It must also be able to restrict access to information found by the search (at least on a document level, if not on a field level).

Individual agencies will determine information to be shared and decide upon the mechanisms for which the JUSTIS System will acquire the shared data. Information detailed in the following section is a result of vision and information gathering interviews conducted with the individual agencies.

3.2.1 Metropolitan Police Department

The Metropolitan Police Department has chosen to share the following data:

Metropolitan Police Department Shared Data
Identification Data
Last Name
First Name
Aliases
PDID
SSN #
CCN #
FBI #
Address
Date of Birth

Metropolitan Police Department Shared Data
Sex
Race
Ethnicity
Height
Weight
Eye Color
Hair Color
State
Apartment Number
Place of Birth
Citizenship
Scars
Marital Status
City
Zip
Extended Zip
Arrest Data
Arrest Number
PDID
Arrest Date
Arrest Time
PSA
Date of Birth
Race
Sex
Ethnicity
Release Type
CCN
Charge Code
Charge Text
Victim Age
Victim Sex
Victim Race
Booking Date
Booking Time
Booking Location

The selected-shared data are indexed by the following data elements:

Metropolitan Police Department Shared Data Indices
PDID
Warrant Number
Arrest Number

The conceptual MPD participation with the JUSTIS System is shown below.

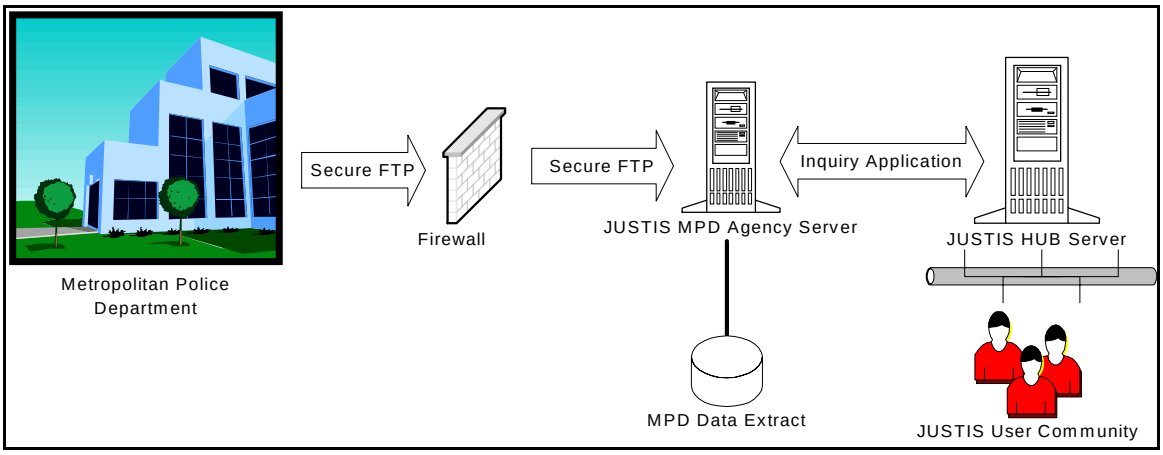


Figure 6 – Conceptual MPD Participation with JUSTIS

3.2.2 CSOSA – Pretrial Services Agency

Court Services and Offender Supervision Agency (CSOSA) – Pretrial Services has chosen to provide an SQL database that will provide an intermediary interface between the legacy systems and the JUSTIS System. The database will provide the following data, which has been agreed to be shared by the Pretrial Services Agency.

CSOSA – Pretrial Services Agency Shared Data
DCDC
PDID
Last Name
First Name
Middle Initial
Date of Birth
Sex
Race
FTD
Parole Ending Date
Parole Status
Hearing Date
Hearing Outcome
Consideration Description
Disposition Description
Disposition Date
Jurisdiction
On After Date
Parole Officer Name
Unit Description
Parole Officer Phone Number
Class Description

CSOSA – Pretrial Services Agency Shared Data
Warrant
Warrant Date Issue
Warrant Date Termination
Termination Description
Release Date
Housing Street
Housing Quadrant
Housing Ward
Housing City
Housing County
Housing State
Housing ZIP
Phone
Case Number
Date Sent
Offender Description

This data are indexed by the following elements:

CSOSA – Pretrial Services Agency Shared Data Indices
Name
DCDC Number
Social Security Number
Aliases
FBI Number
PDID
Interstate Compact Number
BAID Number

The conceptual CSOSA – Pretrial Services Agency participation with the JUSTIS System is shown below.

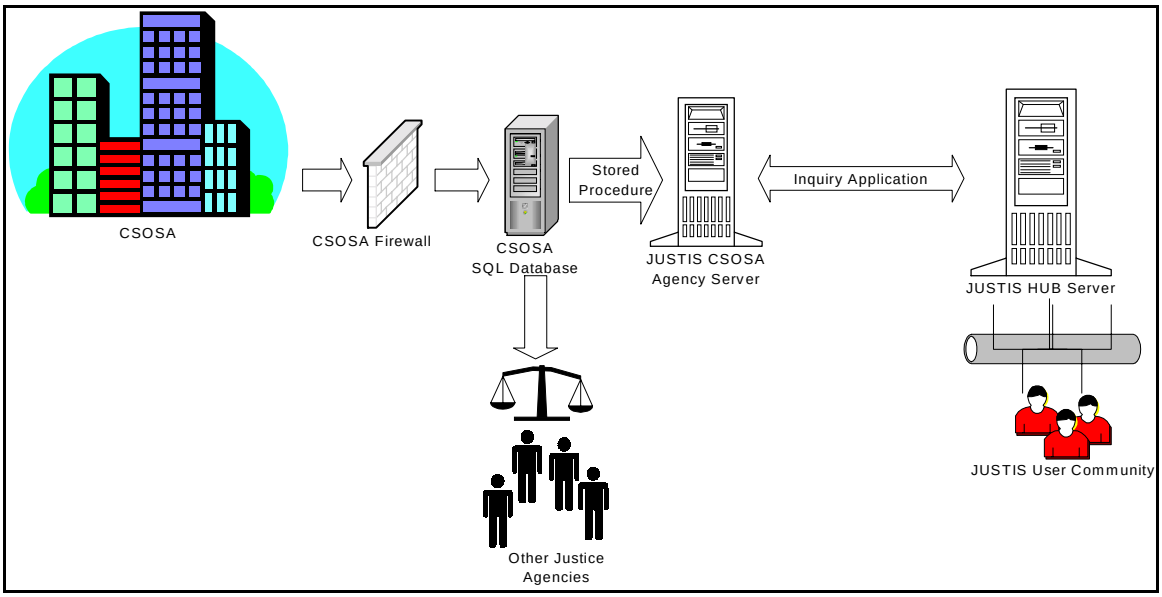


Figure 7 – Pretrial Services Agency JUSTIS System Network Integration

3.2.3 CSOSA – Community Supervision (D.C. Parole)

CSOSA – Community Supervisions (D.C. Parole) will use the same SQL database provided by CSOSA – Pretrial Services Agency. This database will provide an intermediary interface between the legacy system PARIS and the JUSTIS System. The database will provide the following data, which the Parole Agency has agreed to share.

CSOSA – Community Supervision (D.C. Parole) Shared Data
Parole Length
Parole Violations

This data are indexed by the following elements:

CSOSA – Community Supervision (D.C. Parole) Shared Data Indices
DCDC Number

3.2.4 CSOSA – Community Supervision (D.C. Probation)

This agency is not included in the initial JUSTIS Implementation.

3.2.5 Public Defender Services

The Public Defender Services has selected the following data to be shared through the JUSTIS System:

Public Defender Services Shared Data
Case Number
Case Assignment

This data are indexed by the following elements:

Public Defender Services Shared Data Index
PDID

3.2.6 Superior Court of the District of Columbia

The Superior Court of the District of Columbia has selected the following data to be shared through the JUSTIS System:

Superior Court of the District of Columbia Shared Data
Case Scheduling data
Charge Data
Sentencing Data
CJIS data
USAO data

This data are indexed by the following data elements:

Superior Court Of The District Of Columbia Data Indices
Name
PDID

3.2.7 District of Columbia Department of Corrections

The District of Columbia Department of Corrections has selected the following data to be shared through the JUSTIS System:

District Of Columbia Department of Corrections Shared Data
Inmate Location
Institutional Infraction data

This data are indexed by the following data elements:

District Of Columbia Department of Corrections Shared Data Indices
PDID
FBI Number
SSN
Arrest Number (Under Review)

3.2.8 Office of the Corrections Trustee

The Office of the Corrections Trustee has no significant information systems that can contribute to the JUSTIS System.

3.2.9 Federal Bureau of Prisons

The Federal Bureau of Prisons elects at this point to be a user/observer of the JUSTIS System, but not a contributor.

3.2.10 United States Parole Commission

The United States Parole Commission has selected the following data to be shared through the JUSTIS System:

United States Parole Commission Shared Data
Final Decision Documents

This data are indexed by the following data elements:

United States Parole Commission Shared Data Indices
FBI Number
PDID
Name
DCDC Number

3.2.11 United States Attorney's Office

The United States Attorney's Office has selected the following data to be shared through the JUSTIS System:

United States Attorney's Office Shared Data
Case Assignment

This data are indexed by the following data elements:

United States Attorney's Office Data Indices
Docket Number

3.2.12 Department of Human Services – Youth Services Administration

The Department of Human Services – Youth Services Administration has selected the following data to be shared through the JUSTIS System:

Department of Human Services – Youth Services Administration Shared Data
Supervision Performance Data

This data are indexed by the following data elements:

Department of Human Services – Youth Services Administration Data Indices
Social File Number
YSA File Number

3.2.13 Office of Corporation Counsel

This agency will not be included in the Blueprint.

3.2.14 District of Columbia Department of Motor Vehicles

This agency will not be included in the Blueprint.

3.2.15 Summary of Data Contribution

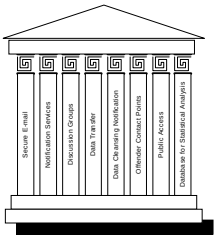
The following table summarizes the data that agencies have discussed sharing and the data that other agencies have expressed a particular interest in.

Data Category	Metropolitan Police Department	CSOSA	Superior Court of the District of Columbia	District of Columbia Department of Corrections	Federal Bureau of Prisons	Unites States Parole Commission	United States Attorney's Office	Youth Services Administration
Identification Data	♣							
Arrest Data (PD163)	♣	♦	♦	♦		♦	♦	♦
Sex offenders Information	♦							
Correction Information	♦							
Charge Data		♣						
Pretrial Release Status		♣						
Warrant Data		♣						
Parole Length Data		♣						
Parole Violations		♣						
Pretrial Drug Test Results		♣						
Case Scheduling Data			♣					
Charge Data			♣					
Sentencing Data			♣					
CJIS Data			♣					
USAO Data			♣					
Lockup List			♦					
Location Information			♦					
Mug Shots			♦					
US Attorney Assignment			♦					
Inmate Location				♣				
Institutional Infraction Data				♣				
US Courts Data				♦				
DC Courts				♦				
Final Decision Data						♣		
Pretrial Data						♦		♦
Per-Sentence reports						♦		
Case Assignment Data							♣	
PD251		♦					♦	
Pretrial Current Status							♦	
Pretrial Condition of Release Data							♦	
Pretrial Probation officer Data							♦	
Social File Number Data								♣
YSA File Number Data								♣
Court Disposition Data								♦
Juvenile Probation Data								♦

♣ – Contributed Data

♦ – Agency Expressed Interest in this Data

3.3 Interagency Functions Supported by the JUSTIS System



The previous section described the core functionality of information sharing within JUSTIS. This section discusses the individual functions that further enhance the system and empower its users to fully collaborate with one another.

3.3.1 Secure Email

The future JUSTIS email system is a closed configuration that provides messaging services exclusively to JUSTIS agencies. As security standards become more pervasive in third-party email products, the system could potentially be opened up to Internet access and be integrated with agencies' existing email environments. The JUSTIS enterprise-wide email system will be designed based on a centralized, secure messaging network to provide restrictive communications for sensitive inter-agency information sharing. The centralized messaging system may be extended to a distributed architecture in the future, as traffic volume, user base, and performance expectations grow and as administrative and security policies are developed.

The initial JUSTIS System email architecture will be centralized to establish secure messaging in a well-controlled environment. The Simple Mail Transfer Protocol (SMTP) will provide the backbone for communications to the JUSTIS hub mail server over the JUSTIS System network infrastructure. Internet Messaging Access Protocol (IMAP4) and Post Office Protocol 3 (POP3) will be used to access the messages from the email server (See section 3.4.3.4 JUSTIS E-Mail Components). The Secure Multipurpose Internet Mail Extension (S/MIME) standard will be used for encrypted messages and attachments.

The JUSTIS Email system will support the following features:

- Text messages
- Binary attachment
- Authentication
- Encryption and digital signatures

The future JUSTIS System will include the capability for users to send one another electronic mail that has been encrypted and digitally signed. In support of this functionality, JUSTIS will require the use of a certifying authority and a public key infrastructure. Secure email includes the certification that Email came from the user who sent it and that its contents were not altered (See section 3.4.1 Full Security Implementation).

An example is illustrated in the following diagram:

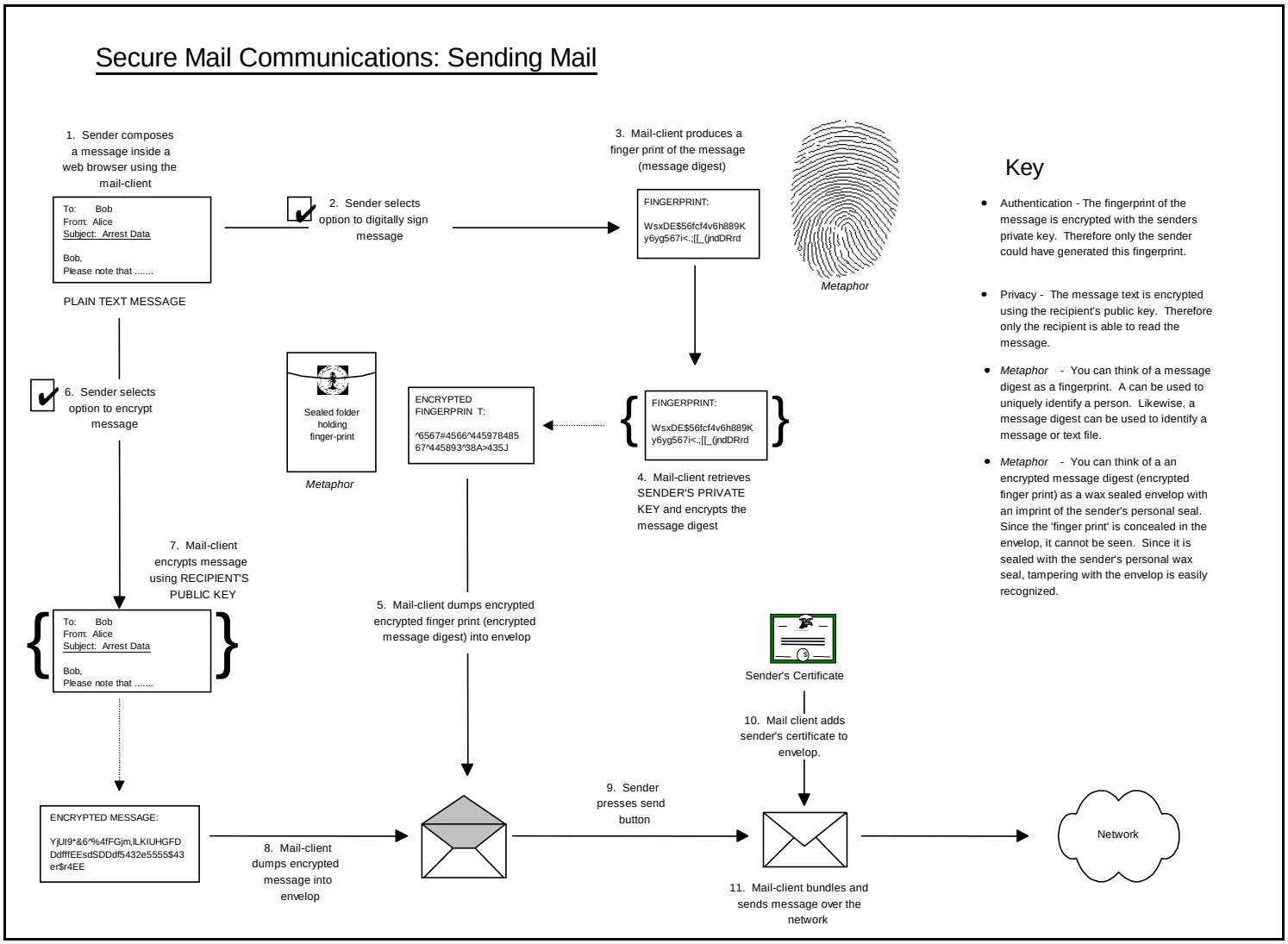


Figure 8 – The Process of Sending Secure Email

3.3.2 Notification Services: Publish and Subscribe

The future JUSTIS System will be designed to allow events within the JUSTIS System to trigger notifications to interested and subscribed parties. The notification could be on an individual basis or a group basis. For example, when a parolee is arrested and booked, this event (the police booking) can generate a notification to a parole officer or group of interested parties. This section of the Blueprint will define major events and those who have expressed an interest in notification.

Below is a summary of the possible events and the corresponding agency that will be notified as a result of the event

Event	Notified Agency
Case Disposition Change	Pretrial Service Agency Probation Agency Public Defender Services DC Department of Correction
Warrant is Issued	Metropolitan Police Department Parole Agency Public Defender Services
Changes in Attorney Assignment	DC Superior Court U.S. Attorney's Office Public Defender Services
Arrest	DC Department of Correction US Attorney's Office
Execution of Warrant	US Parole Commission
Changes to Probation	US Attorney's Office
Parole/Probation Violation	US Attorney's Office
Corrections Release	US Attorney's Office
Changes in Condition of Parole	Youth Services Administration
Client Arrest	Youth Services Administration

The JUSTIS notification function will allow a criminal justice worker to subscribe to a service that will effectively monitor new warrants. As a warrant is issued, the application will "push" a notification to subscribers whose notification criteria include the wanted individual. This notification could be made via secure email. A pager service is used to notify interested parties that a secure notification awaits them in JUSTIS. For example, a Corrections official could register potential and current outside work detail individuals into the JUSTIS System and be notified almost immediately as a warrant is issued against them.

Subscription Process:

- Criminal Justice User Adds, Changes, or Deletes Arrest Notification Subscription using a web browser
- The Subscription update is Acknowledged by the application

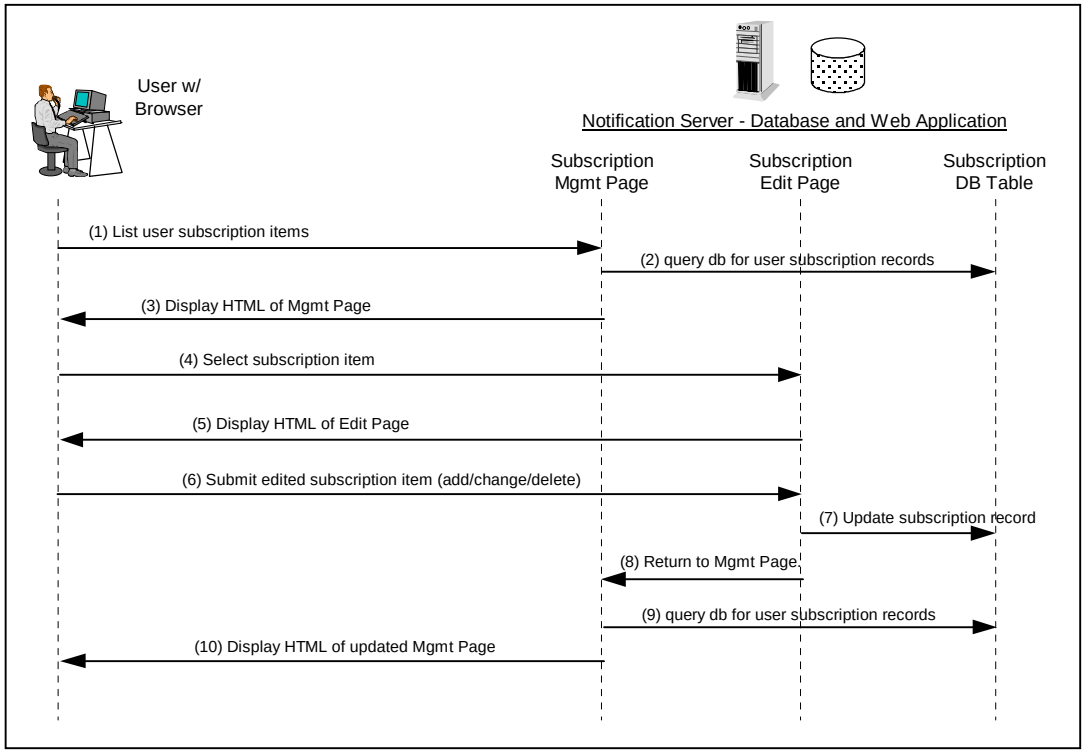


Figure 9 – JUSTIS Notification Services Subscription Process

Subscription Management Page

The subscription management page displays a listing of the user's current subscriptions. A subscription item can be selected to edit the subscription detail. An existing item can be deleted, and new items can be added.

Subscription Edit Page

The Subscription Edit Page is for entering or changing the notification criteria and the notification method. In the edit page the user would specify, for example, the PDID to match to an arrest as it enters the notification system. The user will also be able to choose the notification method – pager and/or email – to be used when a match for the subscription item is found.

Notification Process

- Legacy System sends new arrest to JUSTIS Server
- JUSTIS Server sends notification to Pager Gateway and/or JUSTIS Email Server
- The Pager Gateway sends a Page and/or the JUSTIS Email Server sends a secure electronic mail message to the User.

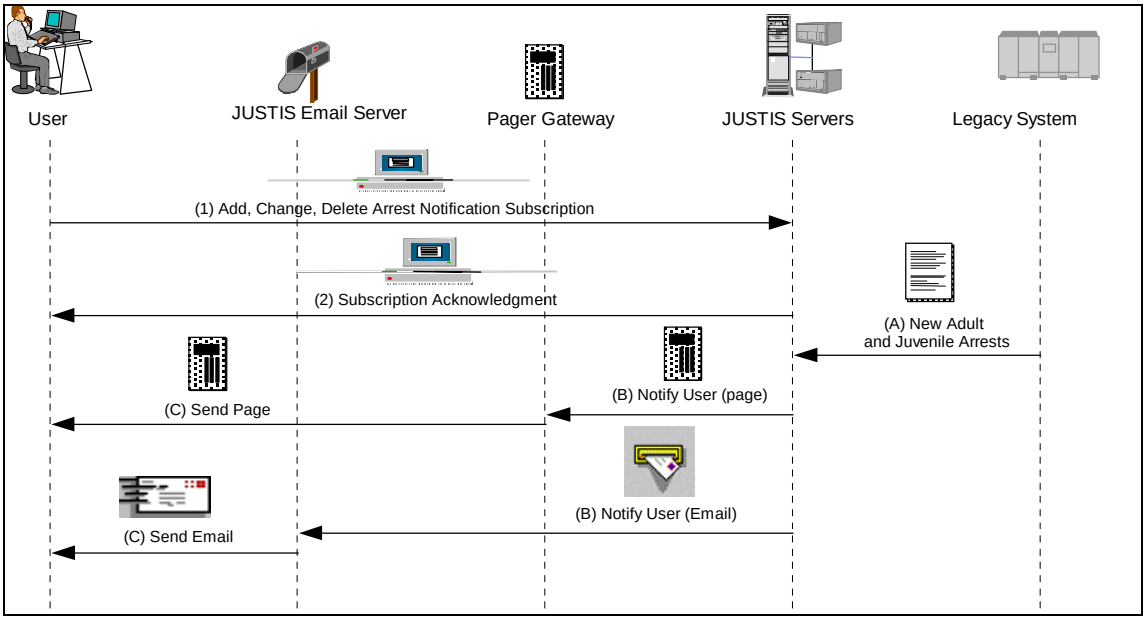


Figure 10 – JUSTIS Notification Process

The electronic distribution is used to deliver information to users desktops automatically without user intervention. It relieves the end users of the retrieval and filtering burden and enables users to have the most up-to-date information without delay. The delivery mechanism is via secure email. Updates can be delivered continuously through a dedicated connection, a preset system interval, or at user-selected intervals.

During final Blueprint preparations, ITAC will need to decide whether JUSTIS should perform notifications on a group basis or individual basis. The decision will be driven by a cost benefit analysis. Individual notifications demand a greater level of system sophistication as well as higher demands for administration and operation of the system. In the end, phased implementation planning may determine to start with group notification and move toward individual notification in a later phase. Knowing this in advance will affect the design of each phase of implementation.

3.3.3 Collaborative Services: Discussion Groups

The JUSTIS System provides the environment for threaded discussion groups/forums. A discussion forum is an on-line conference. A JUSTIS System administrator can set up discussion forums, and any other authorized JUSTIS user with a web browser and the proper access can join in and participate in the forums. Unlike Newsgroups, which are open to the public, threaded discussion groups/forums are only available to authorized users. This on-line forum allows users to:

- Discuss topics of mutual interest.
- Ask questions of anyone in the forum.
- Search through message archives by keyword.

- Accomplish the data cleansing notification system through a discussion group.
- JUSTIS technical help desk questions could be fielded through a discussion group. This would allow both the users and the technical resources to search and review the group's archives for answers to frequently asked questions.

Discussion groups promote a sense of community among members. This capability therefore ties back directly to the JUSTIS business objective of promoting collaboration.

Threaded discussion groups are different from on-line chat. On-line chat takes place in real time, which requires that all participants who want to communicate be logged in and typing at the same time. This makes for a distracting and difficult-to-follow conversation. Threaded discussion groups allow authorized JUSTIS users to view ongoing conversations, post messages to those conversations, and create new conversations at any time convenient to them.

Another difference between on-line chat and threaded discussion groups is that, in on-line chat, once everyone logs off of the chat forum, there may be no record of the conversation. Discussion groups post messages into a discussion database. This allows users to post new messages and view other user's recent and past messages whenever desired. This also allows messages to be indexed and users to search for messages by keyword or other criteria.

Threaded discussion groups are also different from electronic mail. In email, a user's inbox is private to that user. In a discussion group, all members of the group (sometimes referred to as a forum) can see and respond to all messages. The discussion group becomes, in effect, a community in-box.

Discussion groups can be moderated or unmoderated. In a moderated group, a moderator is selected and given special access privileges. When a user posts a message to a moderated group, the message is not made available to the group until the moderator has approved the message for distribution.

The following is an example of the introductory interface of a discussion group:

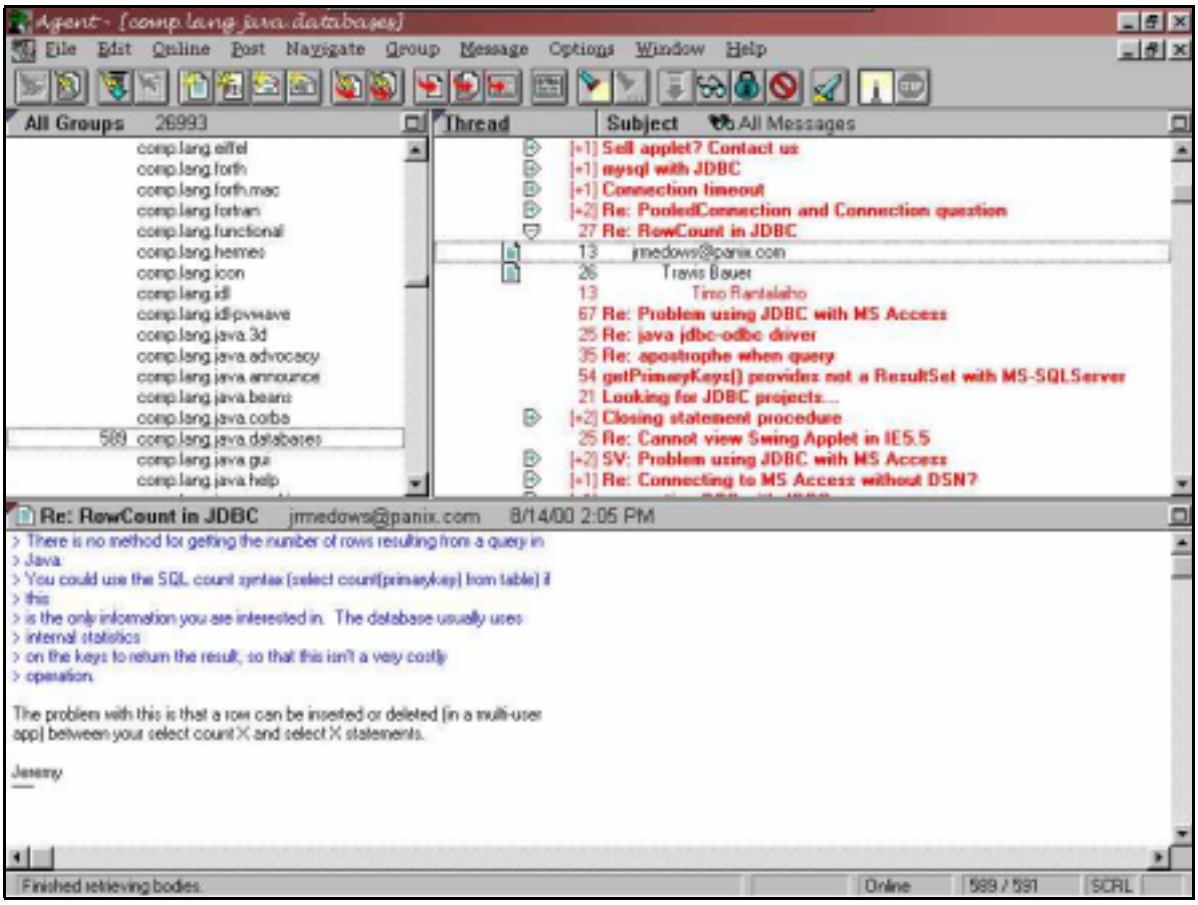


Figure 11 – Screen Capture of a Discussion Group

3.3.4 Data Transfer

JUSTIS member agencies often input a common set of data. For example, first and last names and other identification data are entered in each agency's legacy system. JUSTIS can provide the ability for an agency participant to pull this common data from another agency and use it to populate its new data entries. This function will improve the overall quality and consistency of data that are common to multiple agencies. Sometimes rather than data being pulled, data can also be pushed to participating user and/or agencies. The two approaches are explained below.

Push Technology	Pull Technology
The Server pushes the published content to the Clients	The Clients pull contents from the servers that publish the content
The Server always initiates the data transfer	The Server does not initiates any data transfer through the network until asked to do so

Push Technology	Pull Technology
Sever generates new data according to its own schedule	Clients send requests to the servers directly
Example: PointCast	Example: Software Store

The pros and cons of Push and Pull technology are detailed below.

Push Technology	
Pros	**Cons**
The information is delivered when it is necessary	The Server cannot push data to Clients that connect to network occasionally
The Clients do not have to waste cycles and network traffic to poll servers	Hierarchies may create new requirements for security standards
Servers can better manage the amount of data transferred over the network	Clients get more information than they desire
A hierarchy of Servers supplying the same data can create efficient content distribution and scalable Client/Server implementation	Involves more hardware and software requirements for hierarchical distribution

The pros and cons of pull technology are detailed below.

Pull Technology	
Pros	**Cons**
The client initiates the requests for data transfer directly to the Server	Increases network traffic
The client can filter data that it has requested	Large number of cycles are used to get the data

Another approach can be EDI (Electronic Data Interchange). EDI is commonly defined as the direct computer-to-computer exchange of information or data. EDI bridges the gap between different agencies with different systems. EDI typically includes data formatting and translation. A standard criminal justice file format should be developed to support EDI. A new Internet standard, called eXtensible Markup Language (XML) can also be considered. XML is a set of tags and declarations – but rather than being concerned with formatting information on a page, XML provides information about the data itself and how it relates to other data. In essence, XML is emerging as a standard for web-based delivery of data in an agreed upon structure.

3.3.5 Data Cleansing Notification and Processes

The implementation of a system whereby related information from different sources can be viewed requires a business process that resolves data inconsistencies. By pulling together multiple agencies' views of data through the JUSTIS System, inconsistencies might be noted. The JUSTIS System accommodates a business process whereby the user sends a report via secure email of inconsistencies or suspected errors to another agency's data administrator. The data administrators from the different agencies coordinate a resolution to the data inconsistency. For example, a user retrieves data from MPD that displays an offender's charge number. This same user notices that the data retrieved from Pretrial

Services Agency displays a different charge number. The user could then send a secure email to the data administrators of both systems requesting them to verify the data and correct it accordingly.

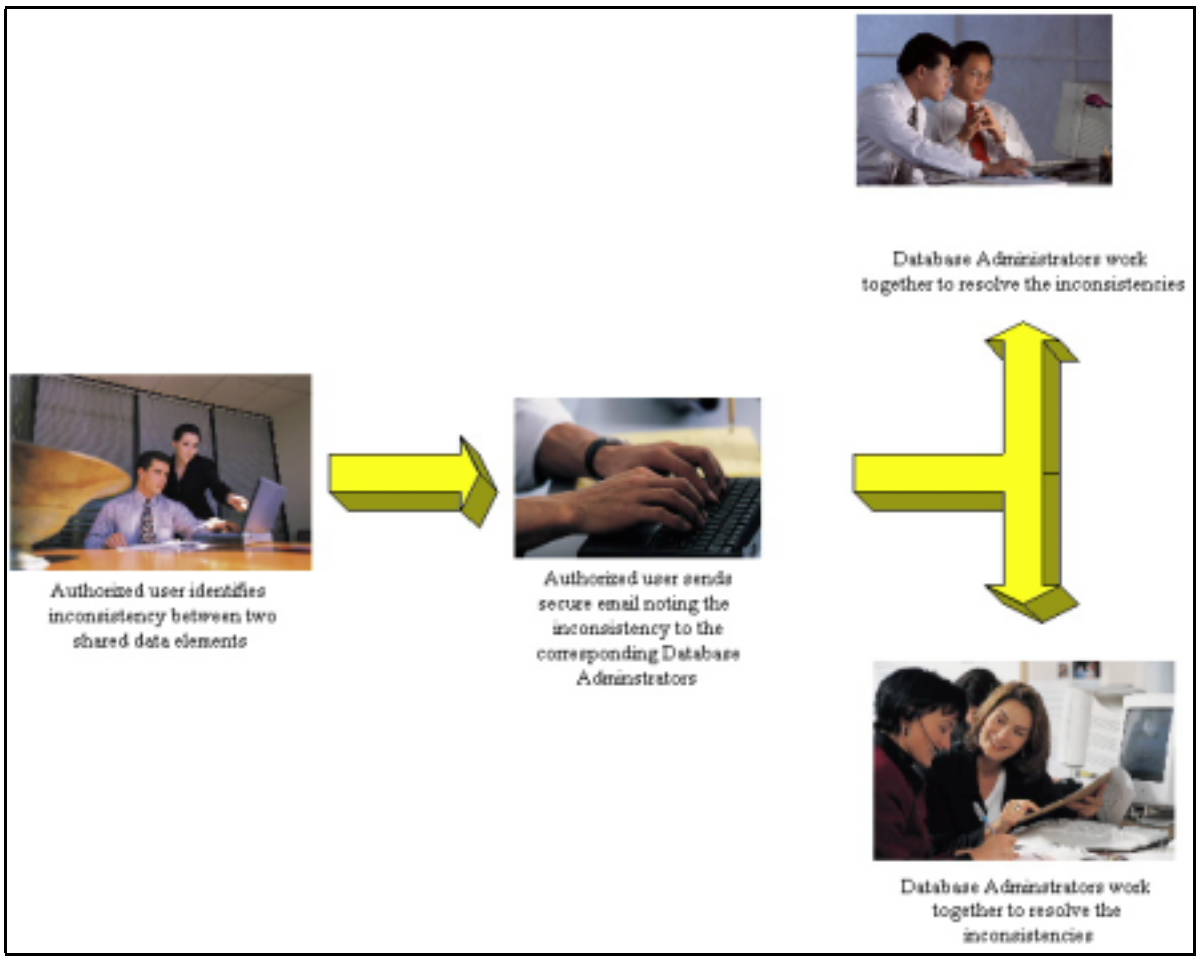


Figure 12 – Data Discrepancy resolution representation

3.3.6 Offender Contact Points

In addition to providing individual agency views of data, JUSTIS can provide a consolidated list of all the agency contacts and their phone numbers as they pertain to an individual case. Thus far, user queries have been returning a single tabbed page for each agency's matching data. For example, a search for John Doe with PDID 123456 will have returned a web page that contains tabs with participating agency data.

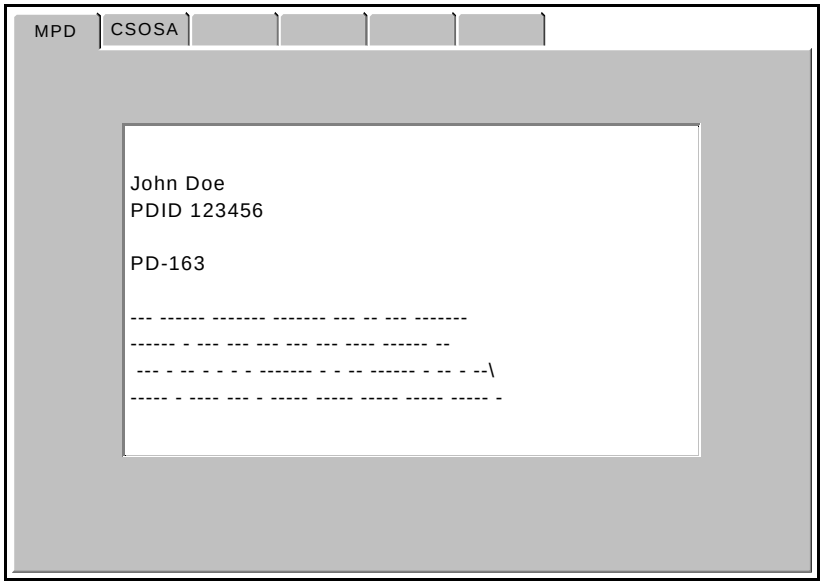


Figure 13 – Tabbed Dialog of Inquiry Application Results

This view is extremely useful and shares the participating agencies data in a logical and easy to navigate manner. The purpose of an offender contact points page is to provide a unified view of all of the various contact persons with whom an offender has a relationship within the justice community. These contacts are brought together and organized on a single page.

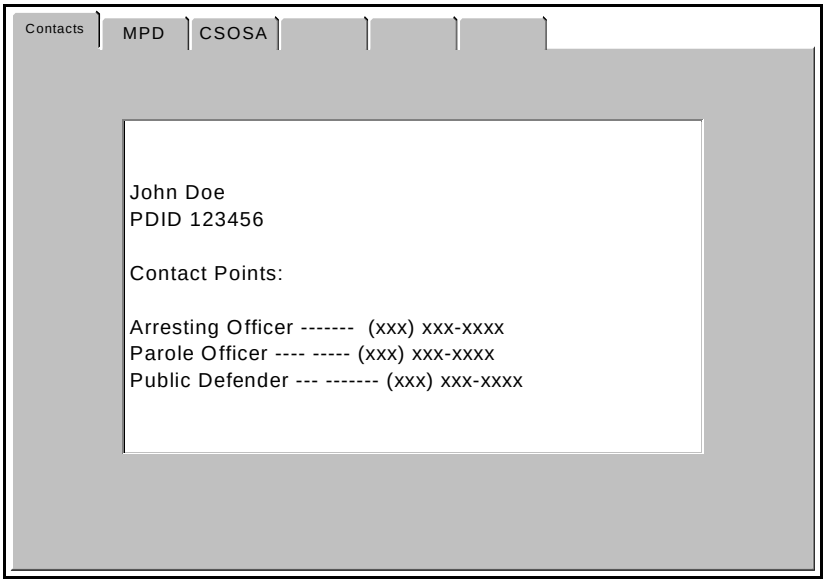


Figure 14 – Tabbed Dialog of List of Contact Points

This consolidated view of the relationships an individual has within the justice community helps to promote the collaboration that is one of JUSTIS's key business requirements.

3.3.7 Public Access

Remaining cognizant of the guiding principles of the ITAC, the JUSTIS System provides the opportunity to "nurture agency and community requirements for research and public access." This principle allows the public to recognize a tangible value from the JUSTIS System. The methodology for publishing data to the public will be exceptionally secure and "one way." The JUSTIS System will publish data in a static format and reports in PDF format that will allow accessibility to the public. As stated before, static format and PDF formats are non-dynamic and cannot be changed due to user input.

3.3.8 Database for Statistical Analysis

Once the JUSTIS System has evolved through a phased implementation, most of the pieces will be in place to allow for the development of a consolidated database and pre-defined as well as ad hoc queries for statistical analysis.

This statistical database is similar in concept to a data warehouse or data mart, and the queries offer similar benefits to data mining. The statistical database we discuss here is based in concept on the Offender Based Transaction Statistics System (OBTS).

In an OBTS the focus is on offender statistics and analysis. The OBTS can contain, in one system, offender data including names and other identifying data, criminal histories, court data, dispositions, restraining and protective orders, incarceration status, probation information, and parole status.

An OBTS is created by transforming a number of data sources through a cascade of processes that result in a unified database for analysis. This process is depicted in the following figure:

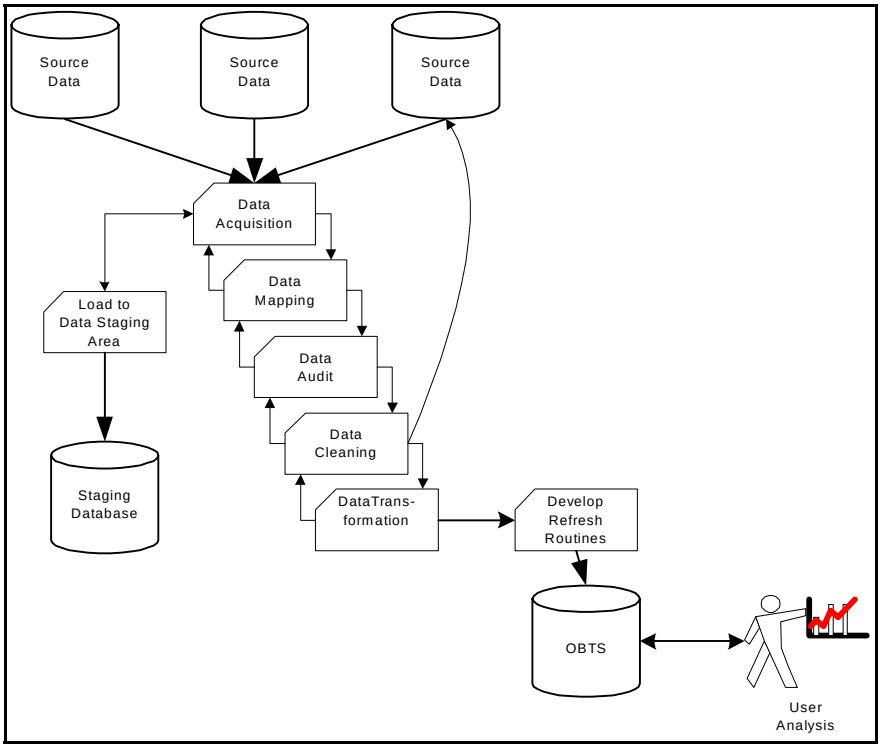


Figure 15 – Statistical Database Creation Process

The above figure depicts the following process flow:

Various **source data** areas are brought together in a process known as **data acquisition**. **Data mapping** takes the format and special meanings of the source data and cross-references them into a common target. For example, database 1 may have a gender code with 1 and 2, whereas database 2 has them as M and F. Mapping would take database 1 and map gender 1 to M and gender 2 to F.

Once the data is mapped and loaded into an intermediate staging area, a **data audit** is conducted. This data audit looks for inconsistencies in the mapped data. For example, 5 percent of database 1 and database 2 records might disagree – one identifies an individual as a male and the other identifies the same individual as female. The data audit produces a series of reports that are used for **data cleansing**. Cleaning the data involves resolving inconsistencies as well as attempting to fill in any missing data. A key component to data cleansing is that it is the source data that get cleaned. If the intermediate staging data were cleaned, then each refresh of the OBTS would reintroduce the problematic data.

Once the data have been acquired, mapped, audited and cleaned, they are put through a **data transformation** process. Data transformation involves loading all of the data into a common database structure. This database structure is organized and indexed in such a way as to make queries both easy to develop as well as highly efficient.

This whole process can be difficult and expensive to develop. It also involves a high degree of skilled labor and specialized tools and techniques. In order to gain some economies of scale, **data refresh routines** are developed. These routines automate the continuing process of keeping the OBTS up to date. Refresh routines typically run once per month or once per week, but can be done more often if greater data currency is demanded.

The resulting OBTS is loaded and routinely refreshed and is now ready for statistical query and analysis.

As was stated in the beginning of this section, JUSTIS will develop many of the necessary components to an OBTS. Specifically:

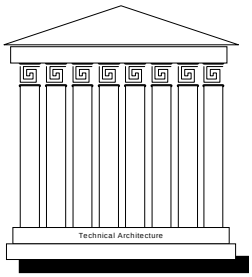
- **Data Acquisition –** the acquisition of data is at the core of JUSTIS' functionality. Data acquired has thus far been in response to user query and have not been stored in any staging area. Nevertheless, automating the acquisition and storage of data would be a natural extension of the capabilities of the JUSTIS System.

- **Data Mapping –** the JUSTIS inquiry applications are built with mapping of data elements as an integral component.

- **Data Audit and Data Cleansing –** A function discussed earlier (See section 3.3.5 Data Cleansing Notification and Processes) was the data cleansing notification feature. This will mean that as JUSTIS is used, users will naturally be conducting an audit as part of their routine operation. Through notification to data administrators, the data will be corrected at the source.

Although many aspects of an operational OBTS will be put in place during phased JUSTIS implementation, there are still a large number of tools and infrastructure components to select and implement. The remaining steps needed to accomplish an implementation of the OBTS will be discussed in the Gap Analysis section (See section 5.2 Identification of Gap Areas).

3.4 Technical Architecture



We have discussed the overall business requirements and system goals of JUSTIS. We then discussed the functional elements of the systems that collectively empower JUSTIS users to achieve the business objectives. This section now turns to the technical infrastructure and architecture necessary to support the functional elements.

3.4.1 Full Security Implementation

The JUSTIS security architecture is modeled after the World Wide Web. Information to be shared will be "published" by its owner agency on distributed JUSTIS Agency Servers, and authorized agency personnel can access JUSTIS server content using web-browser software on a desktop computer. A Hub Server will provide a shared platform for centralized applications, agency-independent content, and inter-agency communication.

Unlike the web, however, JUSTIS will be a secure Intranet. Firewalls will protect the network from unauthorized access. Encryption and digital certificates will provide secure communication and user/server authentication.

The JUSTIS network will be a cooperative and collaborative environment in which many users of the network are interacting at any given time. This interaction requires a strong and flexible layer of security to provide protection to communications over the network and to data stored on the legacy systems.

Security is a collection of technologies that enable JUSTIS to provide and deny access to system resources on a controlled and consistent basis. Security protects the system resources, which can be either physical (network) or informational (application).

The goal of the Full Security Implementation section is to provide a common understanding of the objectives for the JUSTIS Security Framework, the proposed solution, and how the proposed solution works. This section assumes the reader has a working knowledge of client/server applications, web-enabled systems, and a basic understanding of security concepts.

The JUSTIS security framework section is organized into the following major segments.

- Security Framework Objectives – defines targeted objectives for the JUSTIS Security Framework Project.
- Security Concepts – presents an explanation of key security concepts.
- Security Framework Components – covers the main components to the security framework.
- Security Policy – outlines some of the minimum-security policy requirements and considerations in developing security policy.
- Security Summary – Summarizes the full security implementation

3.4.1.1 Security Framework Objectives

The targeted objectives for the JUSTIS security framework are to establish a security infrastructure that supports the following security features:

- **Authentication –** Ability of the system to validate the origin of information or communications.
- **Privacy** – Support for two parties to communicate over a network without a third party being able to observe the communications.
- **Single sign-on** – System to support a user's ability to identify himself/herself and access authorized system resources using a single user ID/password.

In the JUSTIS environment, the above security features will take place between the following entities:

- *Authentication*
  - Client/Server
  - Server/Server
  - Messaging
- *Privacy*

- Client/Server
- Server/Server
- Messaging

- *Single Sign-on*
  - Client to System

3.4.1.2 Security Concepts

In the earlier section we talked about Secure Email. This section will provide an overview of security concepts relating to the JUSTIS Secure Email framework. An understanding of these concepts is crucial to understanding the overall security framework and how it operates. This section will cover the following concepts and terminology:

- Public/Private-Key Encryption
- Message Digest
- Digital Signature
- Digital Certificate
- Third Party Verification

3.4.1.2.1 Public/Private- Key Encryption

Most information transmitted over the Internet or local area networks today is transmitted in plain text, which means that is possible for an unexpected third party to eavesdrop on network transmissions. To guard against possible eavesdropping, encryption can be used to convert information to a format that is difficult or impossible to read (without access to a special key to decode the information). *Encryption* is the process of converting information into data that are difficult or impossible to read. *Decryption* is the process of converting encrypted data back into a readable format.

Public/Private-key encryption is a method of encrypting and decrypting data using a pair of keys: a public-key and a private-key. All users of a public/private-key system are assigned a key pair, where each person's public-key is publicly available, and the private-key is kept private only to the person assigned the key pair.

The public-key and private-key in a key pair are uniquely related in the following way:

Data encrypted with a public-key can only be decrypted with the corresponding private-key.

Therefore, Person A can send Person B confidential information in privacy using Person B's public-key. The only key that will decrypt the encrypted information is Person B's private-key. Since person B is the only individual with access to the private-key, only Person B can decrypt the data and see the confidential information. Data encrypted by a private-key can only be decrypted with the corresponding public-key. Thus public-key encryption ensures privacy.

For example, Person B can send a message encrypted with Person B's private-key to Person A. The recipient of this message (Person A) can decrypt the message only by using Person B's public-key. Since Person B is the only individual with access to the corresponding private-key, Person A validates (authenticity) that the sender of the message is indeed Person B. Therefore, private-key encryption provides a mechanism for authentication.

3.4.1.2.2 Message Digest

A message digest is to a text file what a fingerprint is to a human being. Message digests, much like fingerprints, are used to identify the contents of a particular text file. Computer algorithms are developed to produce message digests such that two message digest are only identical if the two text files are identical.

3.4.1.2.3 Digital Signature

By definition, a digital signature is a message digest encrypted with the sender's private key. Digital signatures fulfill two needs:

- Digital signatures provide a means of authentication through the use of private-key encryption. In other words, digital signatures provide the means to verify the identity of the person who sends a message.
- Digital signatures provide a means to check whether a message has been corrupted during its transmission from sender to recipient.

The following processes described are associated with secure email:

- A digital signature computes a fixed-length string known as a message digest from a message using a hash function.
- The message digest is encrypted with the sender's private-key (ensuring authenticity). The encrypted message digest is known as the digital signature.
- The digital signature is attached to the email and sent to the recipient.
- The recipient decrypts the digital signature (verifying authenticity of sender) to obtain the message digest produced by the sender.
- The recipient uses the same hash function on the message to generate a message digest locally. The recipient compares the message digest sent by the sender against the message digest produced locally. If both message digests are identical, then the message was transmitted without being corrupted. If the two message digests are not identical, then the message was corrupted in transmission. If the recipient is unable to decrypt the digital signature, then the sender was not the person as claimed to be in the message.

3.4.1.2.4 Digital Certificates

A digital certificate is an electronic document that serves as a form of identification. It serves a similar function as any other type of identification, such as a driver's license, or a worker's badge. During client-server transactions and email communications, certificates are exchanged to validate the two parties communicating.

In a certificate-based secure environment, a certificate is installed onto a user's web browser and protected with a user-supplied password. Then at any time a user wishes to access system resources, he/she authenticates himself/herself to their web browser through the use of their username and password. This enables the browser to use the certificate as identification on behalf of the user. The user is then able to access secured system resources. All transactions and exchanges of certificates take place between the web browser and server on behalf of the user. This type of environment offers users the desirable benefit of only requiring the user to know one password.

Certificates are issued to application servers of the system as well as users of the system. This provides users with protection by being able to authenticate a server application before using it. This warns a system user from accessing a fraudulent system resource.

Certificate Authority

A certificate authority is an organization charged with issuing digital certificates. Among a certificate authority's duties is the responsibility to identify the person associated with a certificate and verify that the person is in fact an authorized user of the system prior to issuing certificates.

The duties of a certificate authority are analogous to the duties of an organization responsible for issuing driver licenses. For example, DMV is responsible for issuing drivers licenses in the District of Columbia. Prior to issuing a driver license, DMV has the responsibility to verify the person's identity and verify the person is authorized to and competent in operation of motor vehicles. Upon this verification, DMV issues a driver license to the applicant. In the event a person's driving privileges are suspended, DMV has the responsibility to revoke the license. Likewise, if a person's privileges to access system resources are suspended, then certificate authority has the responsibility to revoke the user's certificate.

The illustration that follows shows an example of a certificate. Some of the information in the certificate has been highlighted in bold text to help you find certain pieces of information. You should be able to discern quickly that this certificate is for a user named Jane Doe, that the certificate is good from November 12, 2000, through November 12, 2001, and that the certificate was issued by a certificate authority known as the JUSTIS Certificate Authority.

Certificate:
Data:
Version: v1 (0x0)
Serial Number: 1 (0x1)
Signature Algorithm: PKCS #1 MD5 With RSA Encryption
Issuer: **OU= JUSTIS Certificate Authority, S= District of Columbia, C=US**
Validity:
Not Before: **Fri Nov 12 2000**
Not After: **Sat Nov 12 2000**
Subject: CN= Jane Doe, S= District of Columbia, C=US
Subject Public-key Info:
Algorithm: PKCS #1 RSA Encryption
Public-key:
Modulus:
00:d0:e5:60:7c:82:19:14:cf:38:
f7:5b:f7:35:4e:14:41:2b:ec:24:
33:73:be:06:aa:3d:8b:dc:0d:06:
35:10:92:25:da:8c:c3:ba:b3:d7:
1f:1d:5a:50:6f:9a:86:53:15:f2:
53:63:54:40:88:a2:3f:53:11:ec:
68:fa:e1:f2:57
Public Exponent: 65537 (0x10001)
Signature:
Algorithm: PKCS #1 MD5 With RSA Encryption
Signature:
12:f6:55:19:3a:76:d4:56:87:a6:
39:65:f2:66:f7:06:f8:10:de:cd:
1f:2d:89:33:90:3d:a7:e3:ec:27:
ac:e1:c0:29:c4:5a:69:17:51:dc:
1e:0c:c6:5f:eb:dc:53:55:77:01:
83:8f:4a:ab:41:46:02:d7:c8:9a:
fe:7a:91:5c

Figure 16 – Digital Certificate Example

3.4.1.2.5 Third Party Verification

Third party verification refers to the process whereby two parties verify credentials using a third party prior to completing a transaction. For example, consider the following scenario where one person wishes to rent a car:

1. A patron wishes to rent a car.

2. An auto-rental service will only rent a car to a patron provided the patron can present a valid driver license.

3. The patron presents his driver license.

4. Upon viewing the driver license, the auto-rental service has one of two options:

   4A. The auto-rental service can TRUST the driver's license since it appears authentic,

   4B. The auto-rental can perform *third party verification* and contact another party that can vouch for the patron's driver license. For example, the auto-rental service could call the state agency in charge of issuing the license to verify the license is valid.

5. After either *trusting* the license presented by the patron, or after performing *third party verification*, the auto-rental service rents a car to the patron.

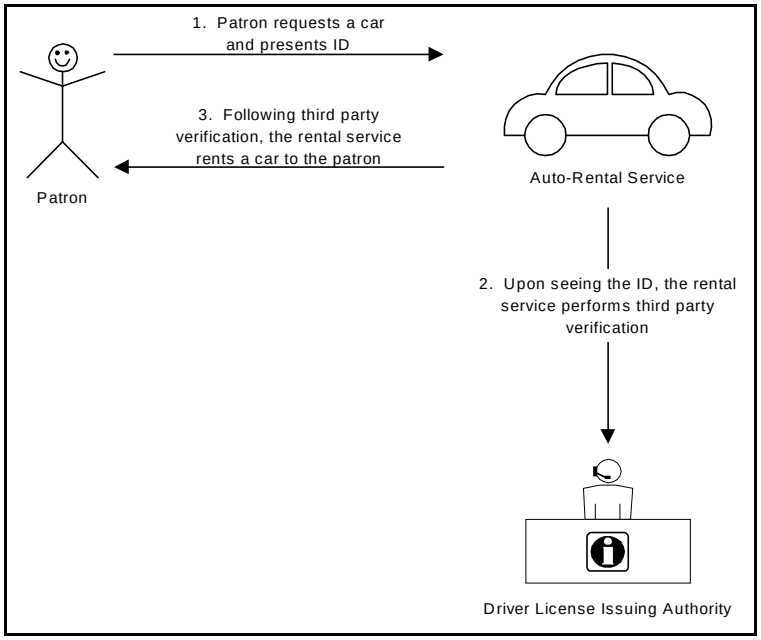


Figure 17 – Third Party Verification Example

Third party verification in a client server environment using certificates is analogous to the example above showing third party verification with a person's driver license

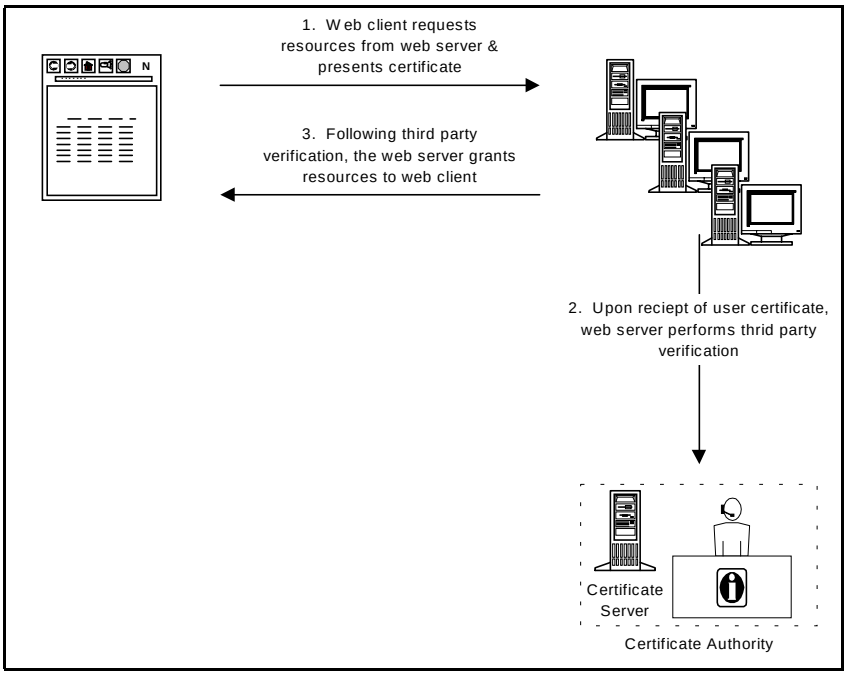


Figure 18 – Third Party Certificate Authority

Summary of Security Concepts

Public/Private-key Encryption – provides a means for privacy and authentication. Private-key encryption is synonymous with authentication. Public-key encryption is synonymous with privacy.

Message Digest – analogous to a fingerprint. A message digest is to a text file (or message) what a fingerprint is to a human being.

Digital Signature – a means of using private-key encryption for authentication in email, and a means to verify whether a message has been transmitted from sender to recipient without corruption.

Digital Certificate – analogous to any other form of identification such as a driver's license. Used in client/server environment to verify identity of system users and system applications.

3.4.1.3 Security Framework Components

There are four major components to the JUSTIS security framework. A description of those components and their major functions as they pertain to security are described below.

- Certificate Authority
- Clients (Web browsers)
- Servers (Web servers)
- Directory Services

3.4.1.3.1 Certificate Authority

The certificate authority is a certification entity responsible for verifying the identity of JUSTIS System users and issue user certificates.

A certificate authority is equipped with a certificate server, which is a server application that creates, manages, issues, and revokes certificates. The certificate server operates in conjunction with other applications to provide a reliable security framework.

3.4.1.3.2 Clients/Web Browsers

JUSTIS users access JUSTIS System resources using a web browser, also known as the client. The clients under consideration for the JUSTIS project are Netscape Communicator and Microsoft Internet Explorer. The clients interact with the certificate server to request and receive user certificates, which in turn are used to identify a user in secure client/server communications.

Users are assigned a single certificate and public-private-key pair following a certificate request. A user fulfills a user-certificate request by filling out an HTML form and submitting it to the certificate server. Following a process conducted by the certificate authority to verify the users identify, the certificate-server issues the user-certificate to the user who in turn stores the certificate in the client (browser). The browser is then able to present the certificate (as proof of the user's identity) to establish secure client/server communication with a web server.

3.4.1.3.3 Servers/Web Servers

Just as web browsers may store certificates to verify a user's identity, web servers can store certificates used to verify the authenticity of another web server. This is desirable because sophisticated users are capable of establishing unauthorized web sites that can mimic an authentic web server, thereby potentially gaining unauthorized information. By establishing web servers with server-certificates, a user on the system can be assured of secure communications. In establishing client/server communications, the web client and server exchange their certificates and then verify each other's certificates against a local database of trusted certificates.

3.4.1.3.4 Directory Services

The directory service is a server application that stores important, up-to-date information regarding users, their contact information, email accounts, and certificates. The directory fulfills numerous critical roles in the systems that include and go beyond the security framework.

In terms of security, the directory is crucial for it is the source of accurate, up-to-date information regarding certificates. Before secure client/server communication can take place, an exchange of certificates must take place between the client (a web browser) and the server (a web server). Once certificates have been successful exchanged and verified between the client and server, a third party verification takes place with the directory server to make certain the certificates in use have not been revoked.

The four components mentioned here, certificate authority, directory services, web servers, and web clients, provide the security framework for the JUSTIS project.

The following diagram illustrates a high level snapshot of the JUSTIS Security framework.

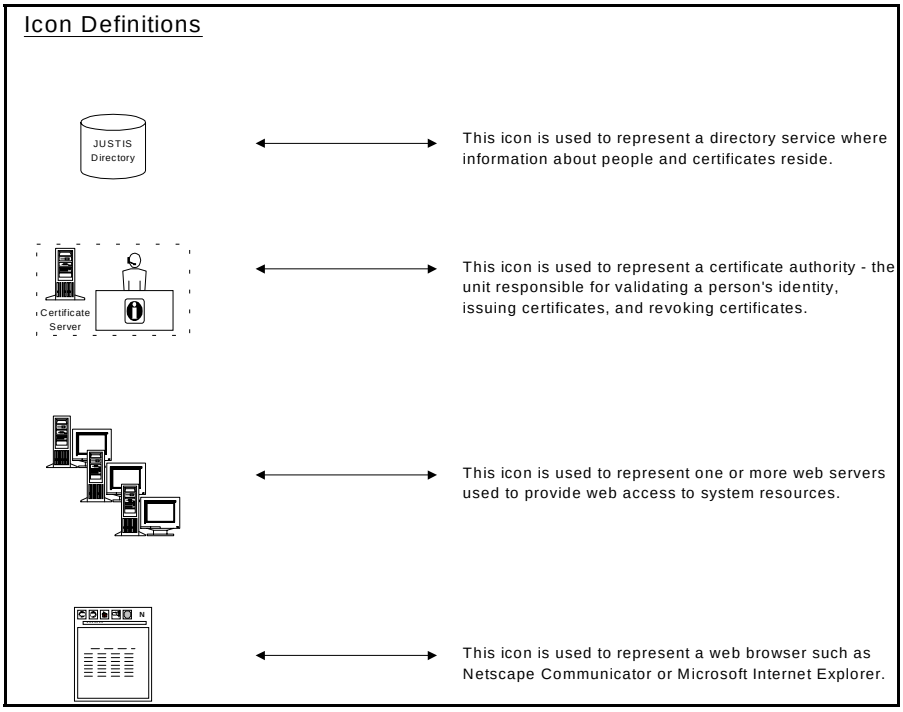


Figure 19 – Security Icon Definitions

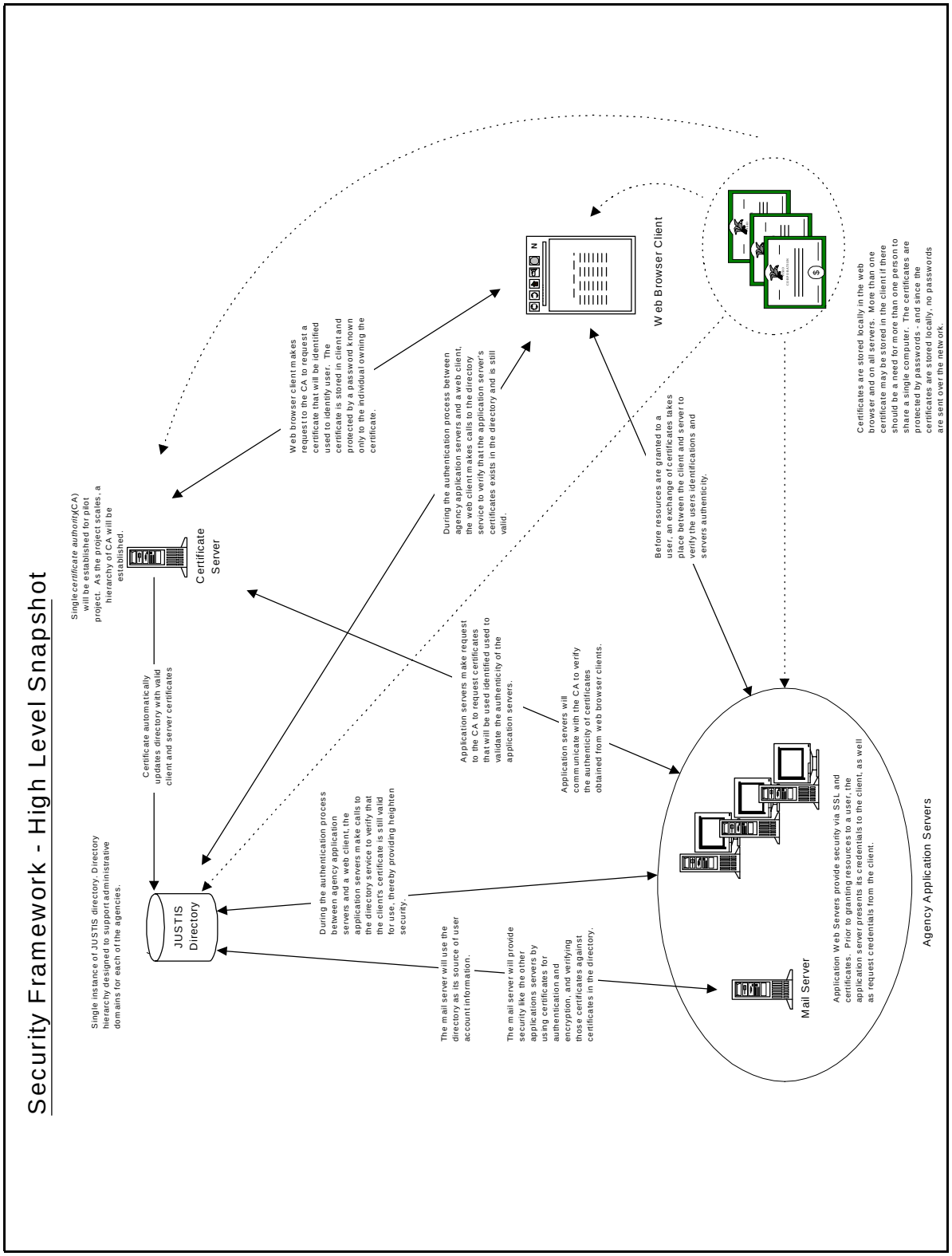


Figure 20 - Security Framework

3.4.1.4 Security Policies

Mitretek – a contractor working on behalf of CJCC – has developed the documents titled “District of Columbia (DC) Justice Information System (JUSTIS) Security Control Requirements”, which addresses security requirements for the JUSTIS System. This document is attached as an appendix to the Blueprint. While the Blueprint has highlighted some of the common security requirements faced when developing a system similar to the JUSTIS System, the Mitretek document addresses all requirements related to the JUSTIS System architecture. Future JUSTIS System functionality will be developed in consideration of Mitretek’s requirements.

3.4.1.5 Security Summary

The overall goal of security is to manage the integrity of these component processes by minimizing, if not eliminating, incidents such as interception of network transmissions or unauthorized use of network resources. This goal is accomplished through the use of supporting technologies such as encryption, dedicated hardware devices such as firewalls, and frameworks such as protocol, digital certificates, and secure systems that blend software and hardware together.

In addition to the technology assurance, the Internet and Intranet security policies that a company embraces are very important. Network security should be addressed from both operational and management perspectives.

Information and resource protection: Authentication and authorization protect the system resources and back end data of an enterprise. Through software such as digital certificates and dedicated hardware devices such as firewalls, the JUSTIS System can prevent unauthorized users from obtaining sensitive information. Using security technologies, the JUSTIS System can also assign various access levels to the information and system resources.

Data Integrity: Hardware and software encryption provide a means to protect data transmission from interception and unauthorized use. Router hardware and software along with secure sockets layer (SSL) and other secure protocols; provide a solid foundation for the enterprise to transmit data securely throughout the network.

Intrusion detection and prevention: The ability to protect a network system from intruders and ensure it 24 X 7 operation is critical in the business environment. Active audits provide real-time intrusion detection and prevention mechanism to protect overall network resources from hackers and unwanted users. Such audits enable the system to block any network intrusion in real time and guarantee to protect data from common network attacks.

3.4.2 Overall JUSTIS Building Blocks: J2EE and Use of Open Standards

As stated in the beginning of this Blueprint, a business requirement of JUSTIS is that it be built upon open standards and technologies. This requirement demands an approach that uses internationally accepted standard tools and techniques. Such tools are available from a wide variety of vendors. Systems developed with open technologies run on a wide variety of platforms.

The use of open technologies is important to the District and to the success of the JUSTIS System. Open technologies offer a number of advantages:

- **Vendor neutrality**. Developers who employ open standards technologies avoid locking themselves into a single vendor. This reduces project risk because a single vendor can fail to fix bugs, slip on release dates or go out of business altogether.

- **Platform independence**. Systems that are developed on open standards technologies are easier to move from one hardware platform to another or from one operating system to another.

- **Greater flexibility**. Because of vendor neutrality and platform independence, JUSTIS participating agencies will have fewer concerns about upgrading their systems and changing platforms. A JUSTIS component built to run on Windows NT and connect to a SQL Server database will require only small modifications to run on a Unix platform connecting to an Oracle database.

The JUSTIS team is developing the system under the Java 2 Enterprise Edition (J2EE) set of standards. The standards selected within this framework are all at an accepted level – no draft standards or vendor extensions have been employed.

The specific standards used to develop and deploy JUSTIS System code are:

- ***JDK 1.3*** – The Java Development Kit, the Java programming language system used to develop JUSTIS application code.

- ***Java Servlets 2.1*** – Servlets are Java code that runs under the control of JUSTIS web servers.

- ***JSP 1.0*** – Java Server Pages are server-processed web pages that include programmatic Java elements.

- ***JDBC 2.0*** – JDBC is the standard access method that connects JUSTIS Java programs with back-end databases.

- ***XML and XSLT 1.0*** – The eXtensible Markup Language and its accompanying style sheet language is a bundle of several related technologies. In JUSTIS, they are used to extend the power of basic web HTML pages.

- ***TCP/IP*** – Transmission Control Protocol/Internet Protocol. TCP/IP is a family of communications protocols that control traffic across the DC Wide Area Network.

- ***HTML 3.2*** – The HyperText Markup Language is what web pages are written in. The version 3.2 standard has been used to help ensure maximum browser independence.

- ***HTTP 1.1/1.0 Hypertext Transfer Protocol –*** This is the standard protocol for transmitting information between browsers and servers. HTTP is a layer above TCP in the protocol stack.

- ***SSL 3*** – ***Secure*** Sockets Layer version 3. SSL enables HTTP and other protocols to be transmitted in encrypted form across a network.

- ***X.509v3*** – ITU-T Recommendation X.509 defines an authentication framework based on digital certificates. The recommendation specifies a set of properties and content for digital certificates, as well as procedures for authentication and certificate management.

- ***X.500 Directory Services***. X.500 is the standard for Directory Services. Directories are essentially databases optimized for read-access of network entity information. JUSTIS uses an X.500 based directory to store information about users, servers, and applications – including group membership and digital certificates – in a centralized location. The Directory Service is available to applications such as web servers and browsers that require identifying information about an entity in JUSTIS. A prime example is a web server that assigns access control to web resources based on group memberships defined in the directory.

- ***LDAP Lightweight Directory Access Protocol***. LDAP is a protocol used by applications to communicate with the Directory. Applications are expected to utilize LDAP and the Directory to reduce the redundancy of user information on systems in a network environment.

- ***SMTP, S/MIME, POP3 and IMAP4.*** These protocols collectively provide a secure email environment.

The JUSTIS System is created on according to a classic 3-Tier paradigm. Systems built along this model are inherently more maintainable because they are functionally organized into modular components that can be individually maintained. The 3-Tiers are the user interface tier, the business logic tier and the backend database tier.

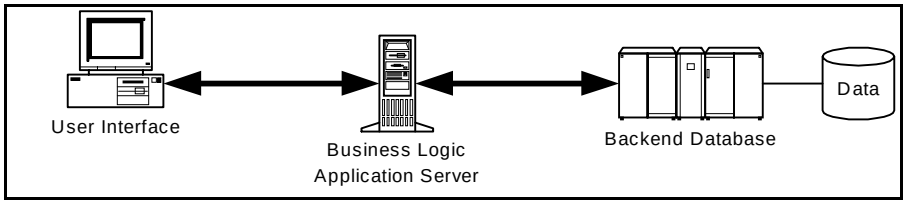


Figure 21 – Three Tier Architecture

.The user interface tier accepts users input (keystrokes and mouse clicks) and displays user output to the screen. In the JUSTIS model, the user interface tier is a standard web browser. Any web browser that can support HTML 3.2 will be able to use JUSTIS. Additional functionality may be delivered to web browsers that are capable of running Java applets. Generally, Netscape version 4 and above and Microsoft Internet Explorer version 4 and above workstations will be able to use JUSTIS.

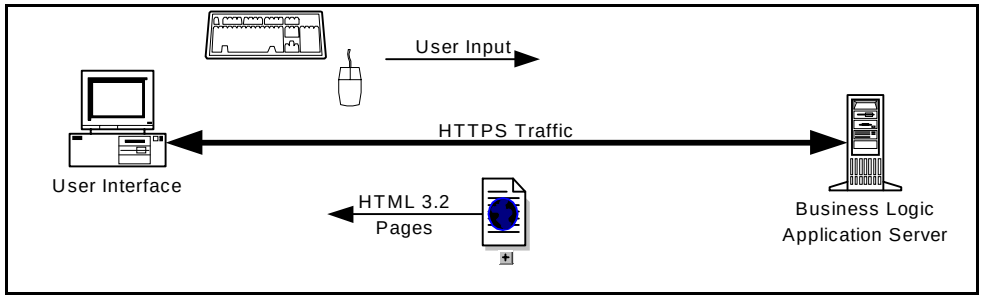


Figure 22 – Communication Between User Interface and Business Logic Tiers

The business logic tier in JUSTIS is a standard web server that delivers standard web pages to the user interface tier. The business logic is built using Java Servlets, Java Server Pages and JDBC connections to

the data tier. JUSTIS is built using Microsoft IIS web server and Allaire's JRun JSP and Servlet engine. The use of open standards means that other web servers and platforms can be used in this tier.

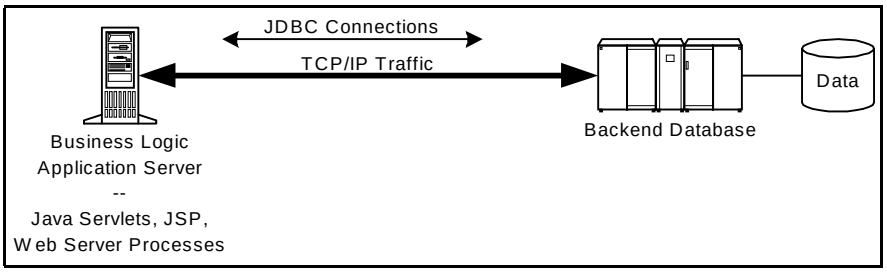


Figure 23 – Communication Between Business Logic and Backend Database Tiers

The backend data tier is under the control of the participating JUSTIS agency. The use of open standards mean that this tier can change with minimal impact on the system. For example, should the database change from SQL Server to Oracle, only one line of Java code needs to change – the one that makes the JDBC connection

3.4.3 Physical Plant Design of JUSTIS Components

3.4.3.1 Overall Architecture

The overall JUSTIS System network is a hub and spoke architecture. The hub components, described below, serve as a centralized traffic manager and offer enterprise-wide services such as email, security certificates, discussion group management and directory services.

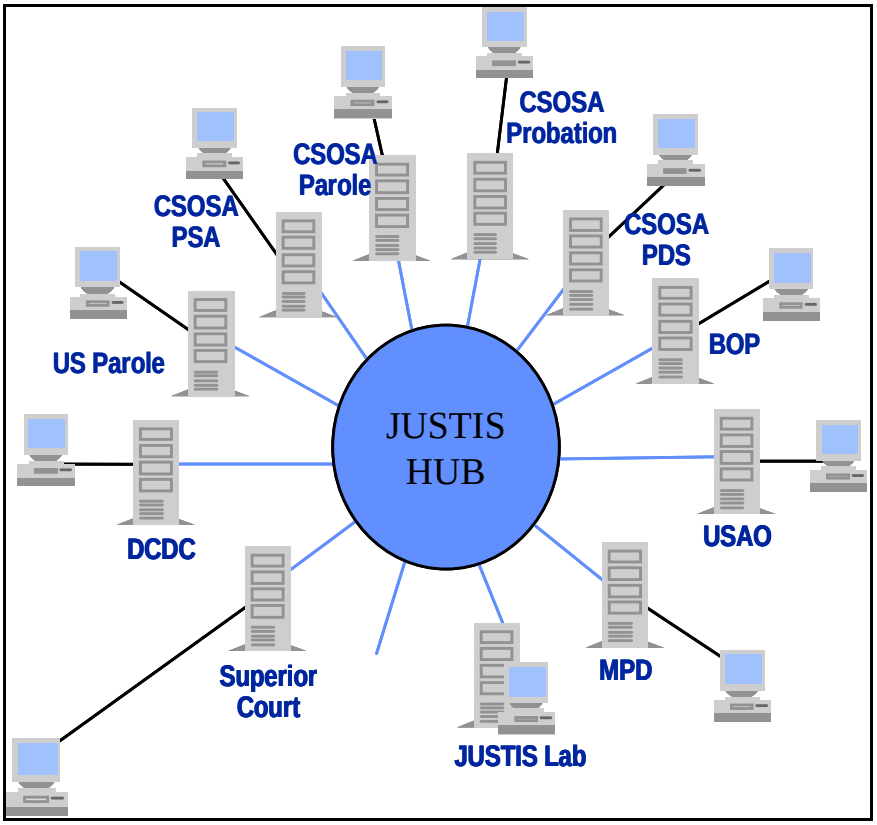


Figure 24 – JUSTIS Hub and Spoke Structure

The spokes of the network are participating agency servers connected to the agency's network, user workstations, and legacy applications and data. Connections are through the DC Wide Area Network using the TCP/IP protocol.

The standards used in the design of JUSTIS leave flexibility in the selection of hardware and software. The details in this section show hardware and software choices that will be compatible with the JUSTIS architecture, but they should not be viewed as absolute requirements.

The server hardware that supports each Hub server as well as each agency server is summarized in the following table:

JUSTIS SERVER CONFIGURATION SPECIFICATIONS
Intel® Pentium® III 933MHz – 2 CPUs
1024MB Total SDRAM 133MHz (2x128, 1x256, 1x512)
Integrated Smart Array Controller (Ultra2)
Hot Plug Drive Cage
RAID 5 setting
36GB Ultra3 SCSI 10,000 rpm Hard Drive – 3 Drives
Hot Plug Redundant Power Supply Module
1.44MB Floppy Disk Drive
10/100 TX UTP
20/40-GB DLT Drive-Internal

JUSTIS SERVER CONFIGURATION SPECIFICATIONS
Windows 2000 Advanced Server
Rack Mountable R1500 UPS (low voltage 100-127VAC)

3.4.3.2 JUSTIS HUB Components

The Hub of the JUSTIS System contains the following servers:

- **Mail Server** – this server provides central support for SMTP, IMAP4 and POP3 services. It supports JUSTIS secure email.
- **Discussion Group Server** – this server provides central support for NNTP services. It supports JUSTIS discussion groups.
- **Certificate Server** – this server is used to assign and maintain security certificates.
- **Directory Server** – this server supports LDAP directory services. It stores user login information, security certificates, email addresses and other directory information.
- **Central Web Server** – The home page of JUSTIS resides on this server. This server serves as a central launching point for the inquiry applications, email, and access to agency web servers and discussion groups. It also provides indexed search of HTML pages and reference libraries on the JUSTIS web and agency servers, as well as search of Internet resources and static web page content such as JUSTIS news, policies, and procedures.

The software components for these servers are:

COMPONENT	STANDARDS/PROTOCOLS	PRODUCT
Web Server	HTTP, HTML, J2EE	MS IIS V 5 with Allaire JRun Server 3
Mail Server	SMTP, S/MIME	Netscape Messaging Server 3.x
Directory Server	LDAP, LDAP API	Netscape Directory Server 1.0x
Discussion Group	NNTP	Netscape Collabra
Certificate Server	X.509v3	Netscape Certificate Server 1.0x

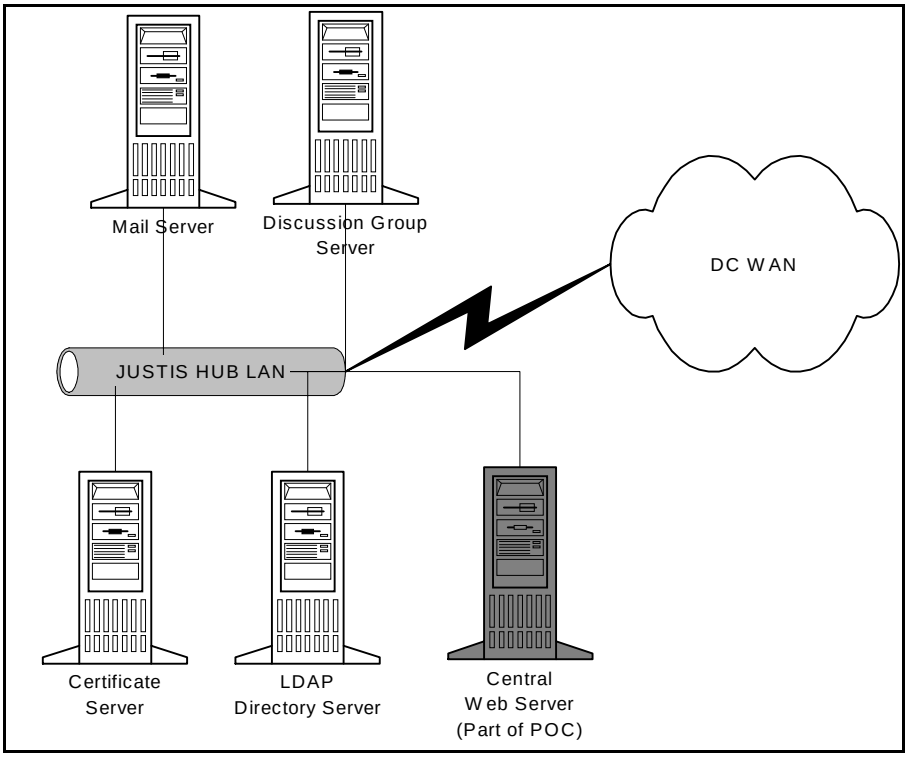


Figure 25 – JUSTIS Hub Components

3.4.3.3 JUSTIS Agency Components

The participating JUSTIS agencies contain one server:

- **Agency Web Server** – The JUSTIS home page of the agency resides on this server. This server serves as the control point for the inquiry applications into the agency's legacy data.

The software components for this server are:

COMPONENT	STANDARDS/PROTOCOLS	PRODUCT
Web Server	HTTP, HTML, J2EE	MS IIS V 5 with Allaire JRun Server 3

3.4.3.4 JUSTIS E-Mail Components

The JUSTIS enterprise-wide email system will be based on a centralized secure messaging network to provide communications for sensitive JUSTIS inter-agency information sharing. Initially, it will be a closed configuration that provides messaging services to JUSTIS agencies only. As security standards become more pervasive in third-party email products, the system may be opened up to Internet access and integration with agencies' existing email environments (if the District adopts common email and security standards).

The initial JUSTIS System email architecture should be centralized to establish secure messaging in a well-controlled environment. However, this centralized system should be scalable to a distributed architecture as traffic volume, user base, and performance expectations grow. The Simple Mail Transfer Protocol (SMTP) will provide the backbone protocol for communications to the JUSTIS Hub mail server over the secure JUSTIS System network infrastructure. Internet Messaging Access Protocol (IMAP4) and Post Office Protocol 3 (POP3) will be used to access messages from the email server. The Secure Multipurpose Internet Mail Extension (S/MIME) standard will be used for encrypted messages and attachments. Intra-agency communications will continue to take place through the existing proprietary mail systems.

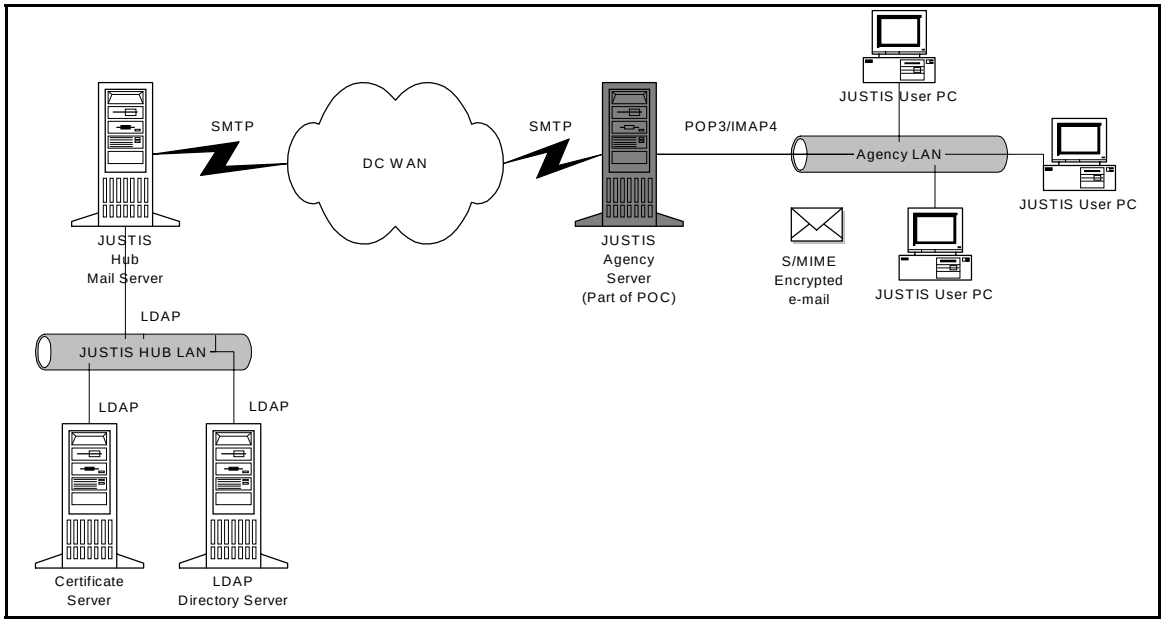


Figure 26 – JUSTIS Email Components

The JUSTIS messaging infrastructure includes the following standards and components:

COMPONENT	STANDARDS/PROTOCOLS	PRODUCT
Mail Client	IMAP4, POP3	Netscape Communicator 4.x Internet Explorer 4.x
Mail Server Administration Server	SMTP, S/MIME	Netscape Messaging Server 3.x
Directory Server	LDAP, LDAP API	Netscape Directory Server 1.0x
Certificate Server	X.509v3	Netscape Certificate Server 1.0x

The JUSTIS mail system will support text messages, binary attachments, authentication, encryption and digital signatures.

3.4.4 Scalability, Performance Requirements

The JUSTIS Proof-of-concept System is required to support fewer than 40 users. However, the design and implementation will allow for scaling to hundreds or thousands of users.

The scalability and performance improvements can be implemented on different components, these are discussed below.

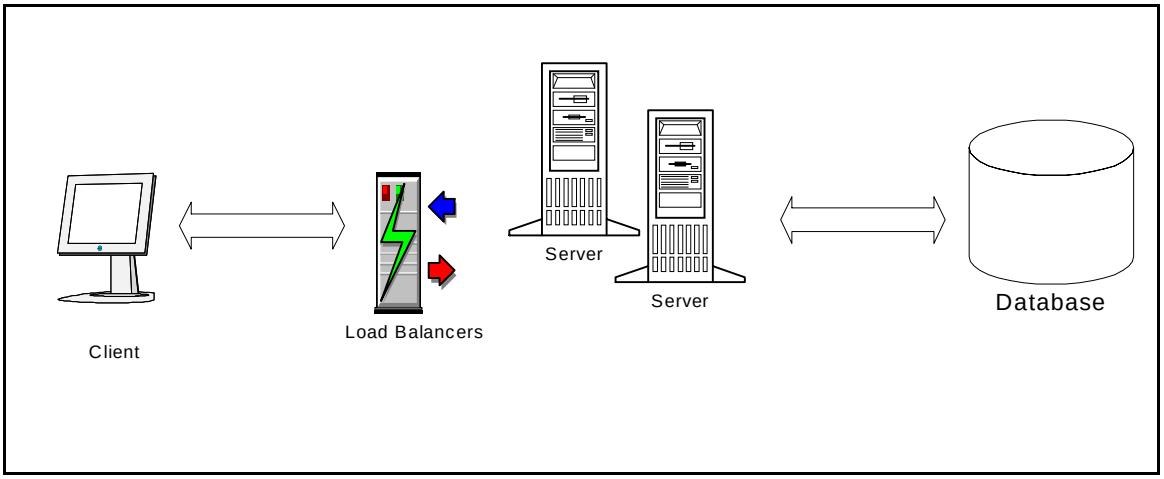


Figure 27 – Areas to Examine for Performance Improvements

Component	Optimizing Technique
Client Side	On the client side, the power of the workstation can be improved by increasing the memory and the processor speed. The disk can be defragmented and the file system optimized
Load Balancers	Load balancers are used between the client and the server, so that the load is distributed equally among multiple servers.
Server	The server side performance improvements can be done be using Servlets and JSP technologies that uses only one active connection to the database for processing the clients request. The use of distributed computing environment increases the performance and scalability to a large extent. Java code can be written to be multi-threaded and to take advantage of multiple processors.
Database	By creating additional indexes on the tables that are queried frequently will improve the performance. Also by running the database in multi-threaded mode will improve performance.
Network	A better network infrastructure will improve the end-to-end response time. Higher speed LAN connections as well as WAN connections can be employed.

3.4.5 User Workstations

The JUSTIS System is a browser-based application; therefore the system has been developed to work effectively with the following components:

- **Network** – Currently the JUSTIS POC is hosted by the District of Columbia's Office of the Chief of Technology Officer (OCTO), therefore users of the system must have a connection to the District of Columbia's Wide Area Network in order to gain access to the system. Similarly, if it is determined to develop the JUSTIS System on a separate wide area network, all users must have access to the network.

- **Browser** – Internet Explorer 4.0 of higher or Netscape Navigator 4.0 or higher. JUSTIS works most effectively with Internet Explorer, due to techniques employed in the District of Columbia OCTO Web Development Kit.

- **Computer Processor** - 486DX/66 MHz or higher processor

- **Operating System** – Windows ME, Windows 95, Windows 98, Windows 2000, or Windows NT 4.0.

- **Memory** - For Windows 95, Windows 98, and Windows 2000: 16 MB (megabytes) of RAM minimum. For Windows NT: 32 MB of RAM minimum

As stated before, the JUSTIS System is designed to be a secure intranet. This requires security components in a browser that may not be included in the version currently residing on a users' system. The users' browser is required to have 128-bit encryption strength. Future JUSTIS functionality may require cookies or JAVA applets.

3.4.6 Network Infrastructure: Special Security Considerations

Mitretek has developed the JUSTIS System security requirements in the document titled, "District of Columbia (DC) – Justice Information system (JUSTIS) Security Control Requirement", that is attached in the appendix of the Blueprint. Future JUSTIS System functionality will be developed in consideration of these requirements. This document addresses network infrastructure requirements such as:

- System Security Plan Requirements.

- Physical and Environmental Protection.

- Operational Controls.

- Integrity Controls.

3.4.7 Application Development Guidelines

Many agencies are in the process of upgrading their individual information systems. Because it is built on open standards according to a 3-Tier paradigm, JUSTIS should be easily modifiable to support changes in the systems to which it connects.

One of the business requirements of JUSTIS is to foster collaboration among its constituents. An element of this collaboration is keeping community members informed of planned system changes. Routine communication of system plans, especially as these plans relate to the interfaces with other agencies and systems, will assist all members of the community in maintaining smooth operation.

Where there is any flexibility in selecting commercial systems or developing custom systems that will interface with JUSTIS, these systems should:

- Store their data in a common, SQL standard relational database management system. Oracle, Sybase, SQL Server and DB2 are currently the four most installed databases.
- The database should support a JDBC driver. Each of the databases mentioned above currently support JDBC 2.0
- The database should support triggers and/or stored procedures. These capabilities will simplify the development of notification services.
- The application should support the export and import of data.
- The platform on which the application resides should support a TCP/IP network connection.
- The application should be web-browser accessible.
- The application should support LDAP directory interaction.
- The application should support the security infrastructure of JUSTIS.

3.4.8 Off-line, Replicated and On-line Data

Acknowledging that each justice agency is independent, it is assumed that each agency's information infrastructure and management is different. These two facts plus the additional fact that the majority of agencies manage a unique legacy system could provide an obstacle when implementing a common information system across the justice agencies. The problem centers around how will the JUSTIS System obtain the agreed upon shared information from the legacy system. The JUSTIS architecture provides three paradigms to chose from in order to accommodate access to agency data.

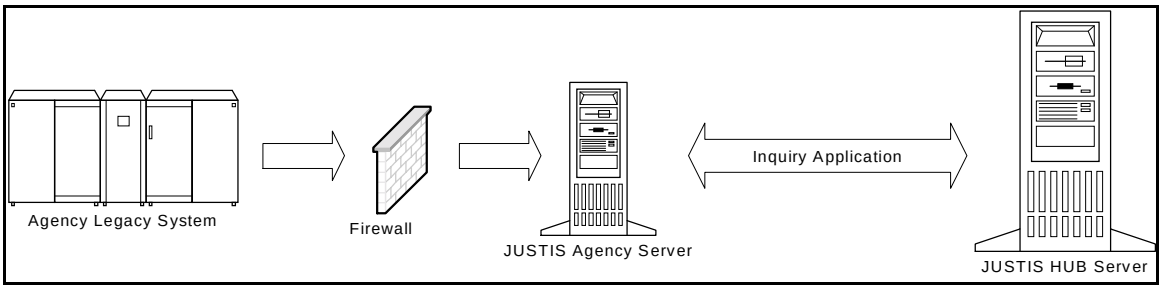


Figure 28 – Direct Access

1. The JUSTIS System can obtain data by directly accessing, in a read-only fashion, that agency's RDBMS database. This would provide the authorized users of the system real-time data retrieval.

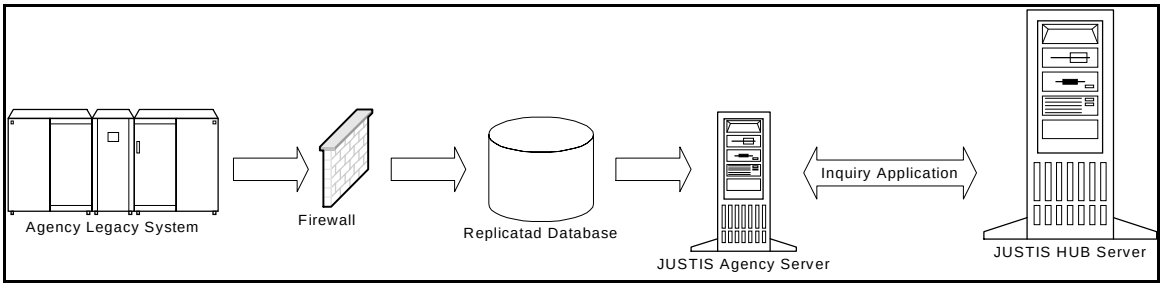


Figure 29 – Replicated Access

2. The JUSTIS System can obtain data by accessing an agency provided replicated database. The data would be updated based upon the programmed schedule of the replicated database.

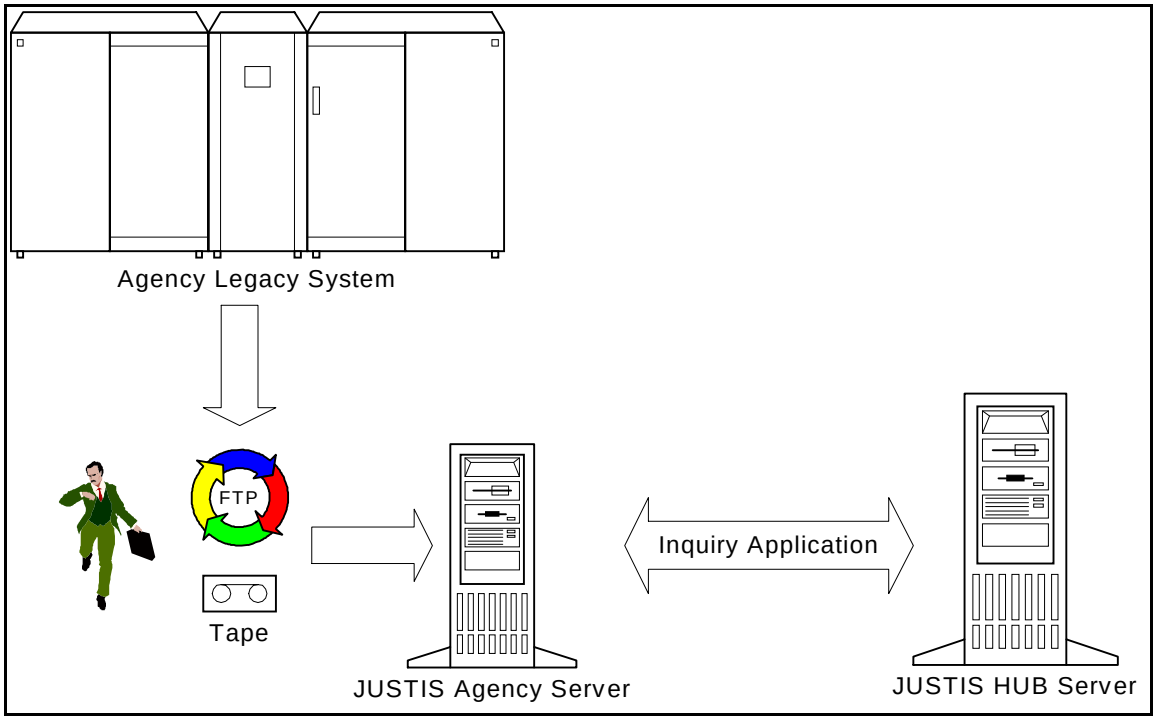
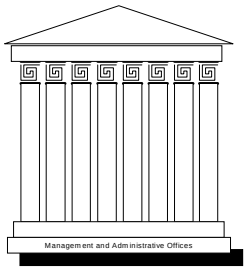


Figure 30 – Off-line Access

3. The JUSTIS System can receive data in an off-line fashion. The data can be downloaded to tape of CD or in FTP format and loaded to the JUSTIS Agency Server. This is the most manual of the three options. This option requires active management of the data transfer. Without active management, data could become outdated, hence ineffective.

Data Access Method	Pros	Cons
1. Direct Access	Real-time Data Retrieval Minimal hardware required Minimal software required	Possible performance impact Possible security impact
2. Replicated Data Access	Data is current Lower performance impact Lower security impact	Higher hardware and software costs Need to maintain data extract programs
3. Off-line Access	Lowest performance impact Lowest security impact	Data is not current Higher hardware and software costs Possible labor-intensive manual processes

3.5 Management and Administrative Structure



We have discussed the overall mission and business objectives of the JUSTIS System. We then discussed the functional elements of the system that collectively empower JUSTIS users to achieve the business objectives. The previous section detailed the technical infrastructure and architecture necessary to support the functional elements. We now turn to the bedrock of our future JUSTIS System Blueprint – the administrative office structure required to support, maintain, enhance and promote the use of the system.

3.5.1 JUSTIS Organization Chart

The JUSTIS System's management and administrative structure can be summarized in the following organization chart:

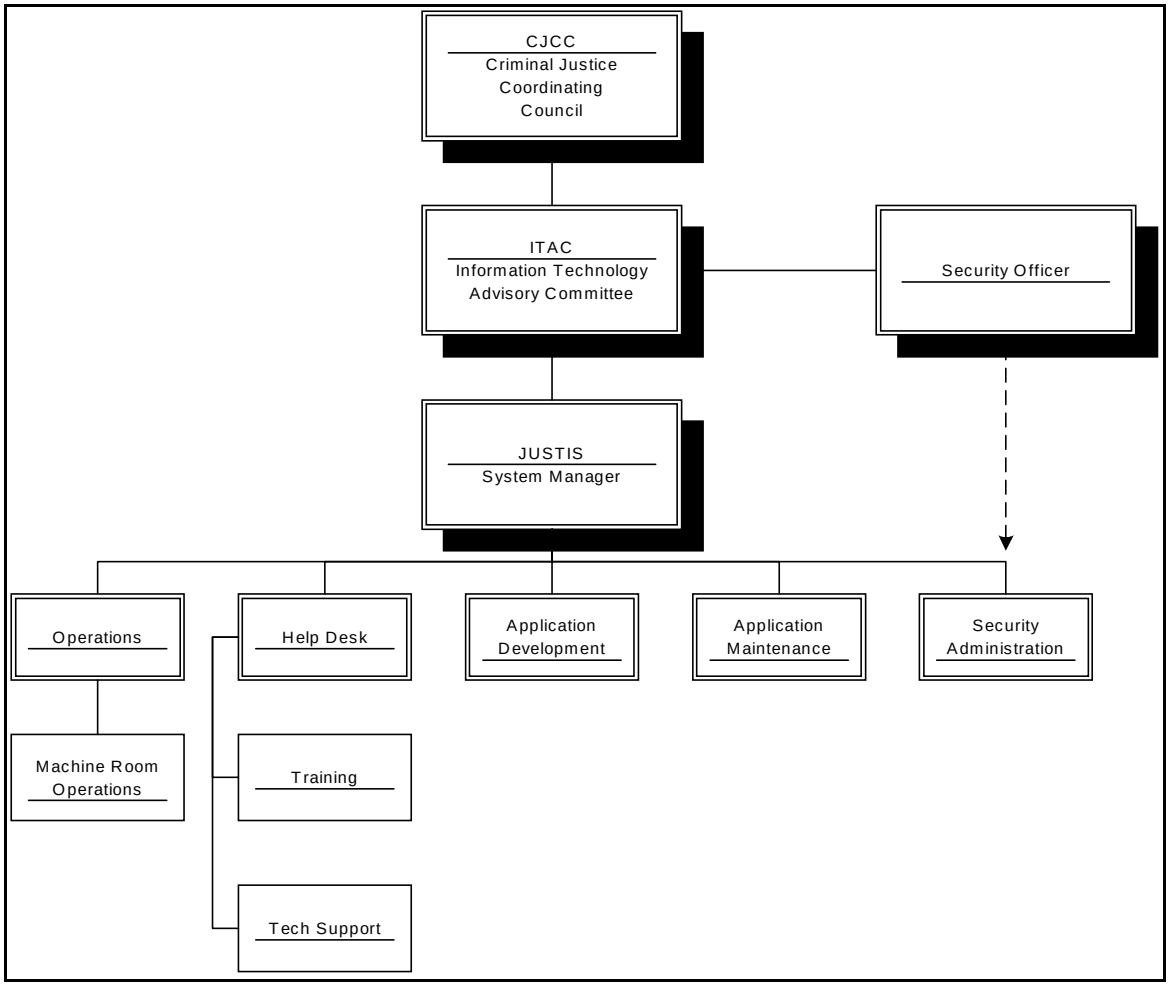


Figure 31 – JUSTIS Organization Chart

The roles and responsibilities of the above organizational members are summarized as follows. These member roles and responsibilities are as they relate to JUSTIS – members have additional responsibilities outside of JUSTIS.

3.5.2 CJCC

The following mission statement comes from the CJCC web site:[3]

> The mission of the Criminal Justice Coordinating Council (CJCC) is to serve as the forum for identifying issues and their solutions, proposing actions, and facilitating cooperation that will improve public safety and the related criminal and juvenile justice services for District of Columbia residents, visitors, victims, and offenders. The CJCC draws upon local and federal agencies and individuals to develop recommendations and strategies for accomplishing this mission. Our guiding principles are

[3] See HTTP://WWW.CJCCDC.ORG

> creative collaboration, community involvement, and effective resource utilization. We are committed to developing targeted funding strategies and comprehensive management information through integrated information technology systems and social science research in order to achieve our goal.

One of the responsibilities of CJCC in conducting its mission is to set the overall direction and mission for ITAC. The CJCC sets ITAC's information technology mission for intra-justice agency collaboration.

3.5.3 ITAC

The ITAC's mission and goals are expressed as follows on CJCC's web site:[4]

> Mission
>
> The Information Technology Advisory Committee shall advise and recommend on matters pertaining to the funding, development, operation, maintenance and monitoring of a Justice Information System to improve public safety and the related criminal and juvenile justice services for the District of Columbia residents, visitors, victims and offenders.
>
> Our guiding principles are to:
>
> - Recognize the primacy of each justice agency mission
> - Facilitate collaborative solutions to justice information challenges
> - Commit to the quality and integrity of justice data
> - Implement effective data and system security
> - Respect the confidentiality of information and individual privacy
> - Establish of system-wide standards, supported by common identifiers and positive identification
> - Nurture agency and community requirements for research and public access
> - Provide for long term performance monitoring and evaluation
>
> Goals
>
> - Encourage participation by all appropriate District and Federal justice and allied agencies at city and federal levels, including but not limited to, those on the Criminal Justice Coordinating Council

[4] *Ibid.*

- Coordinate and facilitate all aspects of the development of the Justice Information System through careful monitoring and policy decisions and by offering guidance and recommendations to the CJCC and its participating agencies
- Establish and monitor ad hoc and permanent work groups and subcommittees as necessary to address the administration, funding and development of infrastructure technology, data sharing, access, integration, data and system security, system wide standards and measurement of data use and quality, as appropriate to the then-current developmental stage of the justice system
- Communicate the activities and accomplishments of the ITAC, and those units it has established, and the member agencies of the CJCC

In effect, the ITAC carries out the mission it is given by CJCC and has the responsibility to:

- Identify the community expansion of JUSTIS participants
- Identify the functional expansion of JUSTIS capabilities
- Prioritize the order of implementation of the above expansions
- Monitor the implementation of JUSTIS
- Manage the JUSTIS System Manager

3.5.4 JUSTIS System Manager

This individual is responsible for:

- Communicating the goals and objectives of the ITAC to the JUSTIS organization
- Managing systems upgrades and implementation
- Managing system quality
- Managing system performance
- Communicating system events and status to the ITAC
- Continued monitoring of legislative actions that could affect the deployed JUSTIS System or allow for increased information sharing opportunities
- Continued monitoring of opportunities for increased system functionality
- Maintaining liaison between all JUSTIS agencies

3.5.5 Security Officer

In order to enforce security and carry the next critical projects forward, a key organizational stakeholder needs to be identified as the Security Officer. METAGroup has identified this as a critical component to

successful implementation. They note that fully 58% of organizations have a central security office and a security officer who reports directly to the CIO.[5]

The Security Office promulgates security policy planning and documentation requirements and conducts the following activities.

The Security Office performs a security audit. Typically, outside firms are engaged to perform independent security audits. These firms attempt to compromise the JUSTIS System and report on their findings. The results of the exercise are used to plan strengthening measures for the network infrastructure, data, applications, systems, and facilities.

The Security Office performs a security policy audit. The newly formed Security Office should collect and review all existing security policy statements from all agencies. The Security Office should assume the responsibility of organizing, publishing, managing and enforcing this enterprise-wide security policy.

The Security Office reviews and enhances security infrastructure elements. For example, Firewall policies and standards are an important element of a secure environment. The use of DHCP and non-routable internal IP addresses should also be reviewed to ensure that internal host addresses are hidden from external view through firewall re-mapping.

3.5.6 Operations Department

The JUSTIS System requires a well-trained operations staff for ongoing operations and administration of the system. Operations staff is critical to maintaining the functionality of the system by:

- Maintaining facilities personnel on a 24 by 7 basis.
- Maintaining disaster avoidance practices such as routine backups and preventive maintenance.
- Maintaining disaster recovery practices such as the development and exercise of a JUSTIS disaster recovery plan.
- Monitoring system use and maintaining log files.
- Monitoring system performance.
- Managing hardware and software licenses and maintenance contracts.

3.5.7 Help Desk Department

In order to take advantage of all the JUSTIS System capabilities, it is recommended that users, once granted access, attend training. Also, once the user community becomes sufficiently large, as determined by the ITAC, a help desk will be needed to provide end-user support.

[5] METAGroup Power Summit, Security: The Cornerstone of E-Commerce, June 18, 1999

3.5.8 Applications Development Department

The applications development department will be comparatively large during phased JUSTIS implementation and will reduce in number as the system nears full implementation. A number of roles within this organization might be fulfilled by a single individual. These roles and their duties include:

Web Site Content Originator

The Content Originator creates content and maintains a fresh, valuable, quality electronic information product.

Web Site Content Owner

The Content Owners serve as the experts in a given content area. They have the responsibility of managing and providing updated information for a particular section of the site. The Content Owner is often the Content Originator but should always have review and approval authority.

Web Site Content Authority

The Content Authority approves and prioritizes content change requests. The Content Authority is an essential big picture gatekeeper role in the process and is the one most often overlooked.

Web Site Enterprise Authority

The JUSTIS System Manager is the primary Enterprise Authority for JUSTIS. All Internet content and Web sites must be approved by the JUSTIS Systems Manager.

Implementation Manager

The Implementation Manager assigns technical resources for changes to the Web site. After content is created and approved, the implementation process begins. Depending on the type of content and the work level of the technical team, different people with different skill sets may be required.

Implementer

Implementers prepare content for installation. Implementers include HTML programmers, graphics designers, script writers, and any other technically skilled individuals required to prepare content for installation on the site. They will coordinate with the Content Authority to ensure the original intent is translated accurately to the site.

Web Publisher

The Web Publisher operates and manages the Web hosts.

Java Developer

Java developers create, test, debug and maintain Java programs, Java Servlets, Java Server Pages, Enterprise Java Beans and other J2EE elements.

Database Developer

The database developer works with agency legacy applications database administrators to understand, document and connect to participating agency databases.

3.5.9 Applications Maintenance Department

The applications maintenance department will be comparatively small during phased JUSTIS implementation and will grow in number as the system nears full implementation. The roles and duties are in this department are the same as in applications development.

3.5.10 Security Administration Department

The security administrator is responsible for carrying out the polices and procedures set forth by the Security Officer. The Security Administrator:

- Maintains JUSTIS users by creating, deleting or modifying user accounts and access privileges.
- Liaises with security officers and administrators from JUSTIS agency participants.
- Assists with auditing and monitoring activities.
- Maintains security log file information.

4. Current Systems Summary

In order to implement the JUSTIS System with the functionality described in the previous section "Future JUSTIS User Community and System," it is necessary to recognize what Information Technology (IT) challenges may exist by developing a summary of the current systems operating within the justice agencies. The JUSTIS System implementation team developed a summary of the current agency IT environments by utilizing documentation and conducting interviews with ITAC members and selected justice agency personnel.

- The ITLO provided the JUSTIS System implementation team with documentation that represented proof-of-concept engagement requirements, administrative and technical infrastructure summaries and analyses of justice agency business processes and future plans. The table below summarizes the documentation provided.

Summary of CJCC provided documentation

Title	Description
Agency System/Project Chart	Contains information about all the Agencies – Agency code, System Code and System Name
Agency Desktop/Workstation Summary	Contains information Agencies Hardware and Software information
Agency Network Summary	Summary of Agencies' Network Information
JUSTIS POC Participants	Contains information about POC participants
JUSTIS Expectations and Participants	Information about the Participants Expectations
Deliverables	What needs to be delivered as Proof-of-concept
Governance and Structure	Information about hierarchy of different work group, their purpose and mission
CJCC ITAC	Contains information about Justice Agency Infrastructure Vision
Tracking Number Discussion	Tracking number importance and information about it
CJCC	Interagency Agreement on Information Technology
Draft on National Task Force, Tech and Criminal Justice Information	Report about NTF on Privacy, technology and Criminal Justice Information
Paradigms and Prototypes	Security policy considerations for Justice Agency Executives in DC
Privacy, Technology and Criminal Justice Information	Summary of Survey Findings
The National Consortium for Justice Information	About Information
Judicial Administration	Information about DOJ
Information about Data Access Service Improvements	Status Packet
Business Engineering	Recommendation Workflow and Business Engineering
Project OMNI	Business Engineering As -Is Process Document for MPD operational Processes
Comparisons of Definitions in Title	Table of Comparisons

Title	Description
28 & found in State Laws	
Draft Legislation	CJIS Regulation, State Laws, Recommendation etc
District WAN Scheme	WAN Guidelines and Procedures
Interagency automated Data	A CD containing information about diff agency
Justice Grant Administration	Scope of Work
Tracking Number Utilization	Information about Tracking Number Utilization
Privacy and Security support for DC	Criminal Justice information system Intranet
Preliminary Assessment of MPD Information System	Assessment about MPD Information System
Enforcement assistance Formula Grant Program	DC Strategy of Enforcement assistance Formula Grant Programs
Development of Strategic Investment Plan	Final Project Report
Information Technology Architecture Standards	Guide to Information Technology Architecture Standards

- The JUSTIS System implementation team conducted interviews with each member of the ITAC and selected agency personnel. These interviews were conducted in an effort to gain further detail of current interagency business processes, specific agency IT environment, and key member's JUSTIS System "vision."

- The JUSTIS System implementation team also attended various ITAC work group meeting, namely the Technical Working Group and the Privacy & Security Working Group.

The summary of the current IT environments in each of the agencies will help in identifying the concerns and constraints for those who use, administer and manage these environments. The identification of the concerns and constraints are critical to the development of the roadmap that will define the steps necessary to achieve the future JUSTIS System. This section provides a high-level summary of the current IT environment within each of the criminal justice agencies. This information lays the foundation for defining future directions for the JUSTIS System. This section focuses on three primary areas:

- Security Infrastructure

- Network Infrastructure

- JUSTIS Agency Legacy Applications and Data

4.1 Security Infrastructure

A required functionality of the JUSTIS System is to allow access to criminal justice data. Accessing criminal justice data through a technical architecture such as that utilized in the JUSTIS System requires an emphasis on security. This emphasis is addressed by the CJCC through the development of the JUSTIS System security requirements. It is recommended as an initial step in the development of the JUSTIS System security requirements that a current state analysis be conducted and include a review of current:

- Security Staffing
- Policies
- Procedures
- Guidelines
- Logins
- Data Access Level
- Certification Requirement

The CJCC has contracted Mitretek to develop the Security requirements. The results of Mitretek's work are detailed in the document titled, "District of Columbia (DC) – Justice Information System (JUSTIS) Security Control Requirements", which is included in the Blueprint appendix. Future JUSTIS System functionality will be developed in consideration of these requirements.

4.2 Network Infrastructure

The uniqueness of the relationship of justice agencies of the District of Columbia has lead to a complex web of interconnectivity. District of Columbia agencies are centered around the DC Wide Area Network (WAN), while Federal justice agencies have independent WANs. Although the Federal Agencies each have independent WANs, they also contain connections to the DC WAN. The figure below shows the agency connections.[6]

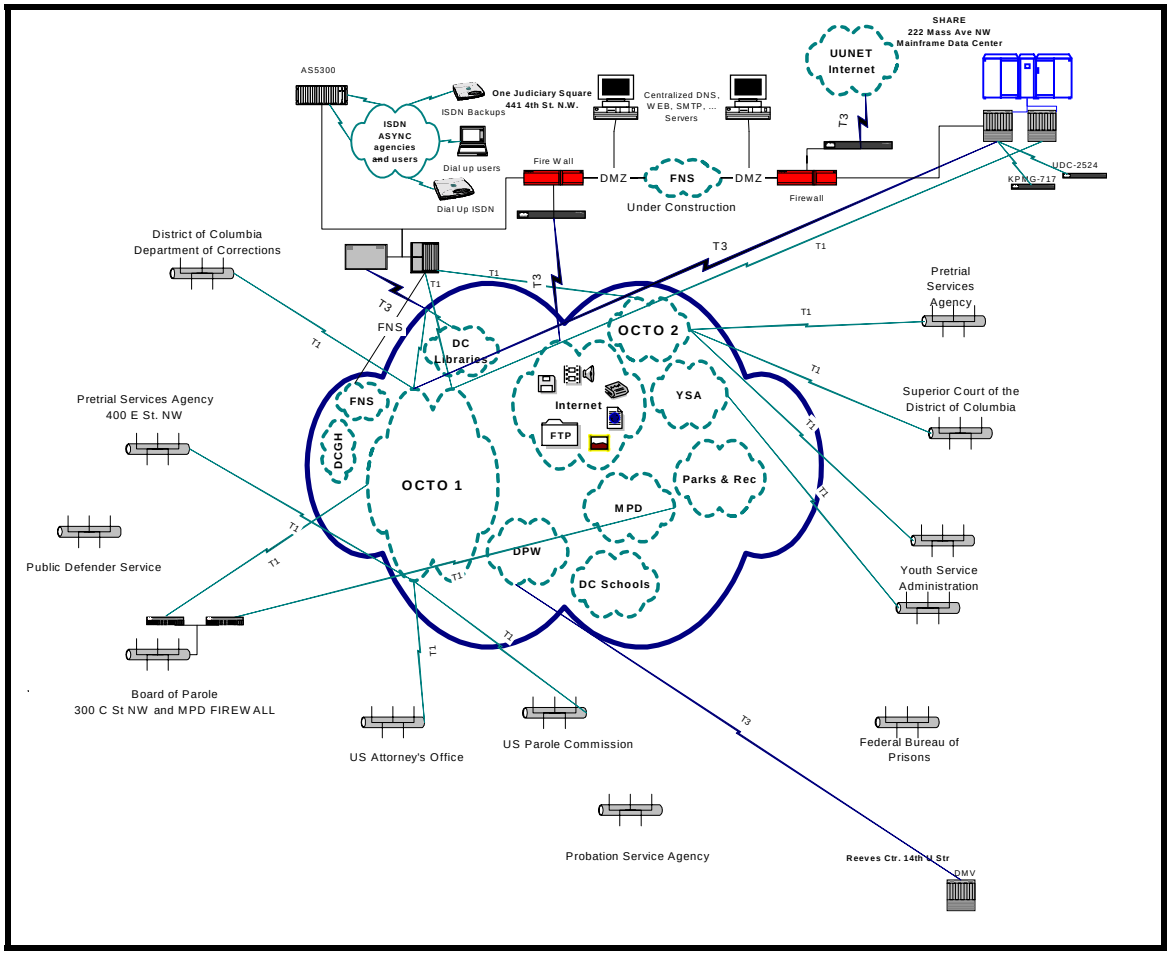


Figure 32 – Justice Agency Connection Points -

[6] This diagram derived from the DC WAN diagrams provided by OCTO.

AGENCY	DC WAN CONNECTIVITY	NETWORK TOPOLOGY	NETWORK HARDWARE	OPERATING SYSTEM	PROTOCOLS	WAN SERVICES	SERVICE PROVIDER	NETWORK SECURITY	MAINTENANCE
Office of the Chief Tech. Officer	6 SMDS Clouds, 464 Sites	Ethernet 10 Base – T Fast Ethernet	Cisco kentrox Digital Line	Novell NetWare 3.12-4.1 3 Servers MS NT Server 4.0 18 Server	TCP/IP IPX/SPX	9.6, 56K,T2, T3 ISDN	Bell Atlantic, UUNET	Cisco Pix 4.25	Internally Managed
Office of Corporation Counsel	T1 1 Site	Ethernet 10Base – T	Cisco Compaq	MS NT Server 4.0 10 Servers	TCP/IP Telnet	N/A	Bell Atlantic	MS Firewall Proxy 2.0	Internally Managed
CSOSA	T1 1 Site	Ethernet Fast Ethernet	Cisco	Novell NetWare 5.0 7 servers MS NT Server 4.0 20 Servers	TCP/IP IPX/SPX	Bell Atlantic Point to Point T1 fiber	UUNET	Secure Firewall Borderware	Internally Managed
DC Dept. of Correction	T1 25 Site	Ethernet Fast Ethernet	Cisco	20 Novell NetWare 4. 1 servers MS NT Server 4.0 5 Servers	TCP/IP IPX/SPX	Bell Atlantic T1	Bell Atlantic	Novell Firewall Border Messenger 3.0	Outsourced
DC Superior Court	T1 1 Site	Ethernet 10Base –T Fast Ethernet	Cisco Compaq Dell	Novell NetWare 4.0 1 Server MS NT Server 4.0 16 Server	TCP/IP IPX/SPX NetBEUI	Bell Atlantic T3	World Com MCI UUNET	Borderware	Internally Managed
Metropolitan Police Department	T1 25 Sites	Ethernet Fast Ethernet 10Base –T Gigabit Token Ring	Cisco 3Com	Novell NetWare 5.0 38 Servers MS NT Server 4.0 7 Servers Unix 6 servers	TCP/IP IPX/SPX	Bell Atlantic T1 9.6 56K	Digex	Checkpoint Firewall 4.0	Internally Managed
Public Defender	T1	Ethernet 10/100	Cisco	Windows NT Server 4.0	TCP/IP	Bell Atlantic T1 – 3	UUNET	MS Proxy 2.0	Internally Managed
US Attorney		Ethernet	Cisco	NT 4.0 Unix Servers	TCP/IP Telnet	Sprint ATM	Sprint	Raptor Firewall	Internally and Outsourced
US Parole Commission	T1		Cisco						
Youth Services Administration		TCP/IP	Cisco	MS NT Server 4.0 9 Servers		Bell Atlantic T1 and 56 K		Cisco Firewalls	

4.3 JUSTIS Legacy Applications and Data

This section provides a summary of the hardware, software, and database management systems in use at the justice agencies. This section also contains a high level summary of the data stored and managed in the information systems within the justice agencies.

The table below lists justice agency and their corresponding information system(s)[7].

Agency Network Summary

AGENCY	SYSTEM NAME	DESCRIPTION
Court Services & Offender Supervision	Automated Bail Agency Database	Defendant database with 250K + names with 12K active.
	Drug Test Management System (DTMS)	Totally automated & Paperless drug testing using barcode
	PRISM	To replace ABA DABA and DTMS
	CSOSA LAN	LAN Connects all CSOSA sites via T1
	Web Server	With dedicated Internet connection w/firewall
	Pretrial – Novel SAA Gateway	Connection to MPD Mainframe
	Probation – PARS	Probation, case workers assignments
	Parole – Parole Information System (PARIS)	Automated parole determination, decision -making
	Parole – Integration of new PARIS with PSA 's PRISM	Integrating the new PARIS with PSA's PRISM and MPD's
	Parole – Image parolee Case Folders	Using the Kodak's Imaging Business Solution software (IBS)
DC Department of Corrections	DOC WAN	16 LAN's with 20 Novell 4.11 Servers, 5 Windows NT4.0
	CRISYS	Inmate records management system includes books
	JALAN	Inmate finance, commissary, and visitation
	New Jail Management System	New System will include CRISYS and JALAN functionality
	Integration with MPD's RMS	To integrate booking, demographics, mug shots, live scan.
	Other Integration Projects	Expected integration with contract facilities.
	Medical Logic	Medical records, appointments, inmate pharmacy
	KRONOS	Automated time and attendance
	HIEDI	Employee substance abuse monitoring
	Lotus Notes	Correspondence tracking, incident reporting and cost auditing
Metropolitan Police Department	Washington Area Law Enforcement System(WALES)	State files & interface for NCIC, warrants, MPD, registration
	Criminal Justice Information System(CJIS)	Criminal history information
	Records Management System (RMS)	Records management, replacement for CJIS/WALES
	Automated Reporting System	Police reporting (UCS reporting software)

[7] This list was completed prior to Y2K system evaluations and also does not reflect development of new systems and elimination of old systems eighteen months prior to August 31,2000. The final blueprint will contain an updated chart.

AGENCY	SYSTEM NAME	DESCRIPTION
	Mobile Data Computers	Laptops in police vehicles
	Message Switch	To handle NCIC communications and data exchanges
	MapInfo GIS	The central crime analysis unit at MPD headquarters
	ArcInfo & ArcView Geographic Information System (GIS)	Intranet map server, distributed capability for districts
	Washington Area Criminal Intelligence Information System	Investigative case management(Homicides, other cases
	Property Evidence Inventory Control System (PEICS)	Records on MPD seized property, contains CCN#s DEA#s
	Time & Attendance Court Information System (TACIS)	Automated capture of MPD employee's time and attendance
	Computer Assisted Dispatch (CAD)	Used for MPD dispatchers, contains a log of calls for service
	AFIS/Livescan	Fingerprint identification system. Mugshot storage system
	Full SUISS	Investigative case management system for all investigated
	FMS (R-Stars)	
	External Interface/Communications Strategy	To eliminate all dumb terminals for desktop applications
	MPDNet	MPD's internal network for desktop applications
	Internet Access	Access to DC WAN
	Desktops	All desktops upgraded to Pentium/NT
	Kiosks & Website	
Office of Corporation Counsel	Case Management and Processing system	Home grown dBASE system currently used
	LAN	No LAN in place this time
Public Defender Services	Network	IBMS AS-400 token ring utilization MS Operating system
	Accounts Payable system	Home Grown System
	Personal System	Home Grown System
	Case Tracking Database System	Home Grown System and used for attorney statistics
DC Superior Court	DC Superior Court Mainframe	IBM ES9121-320, MVS-ESA, CICS, IDMS/R
	DC Superior Court LAN	10/100 Base T with CISCO routers, Bay networks hubs
	Connectivity to the Internet and the DCWAN	To have Internet access email, direct inter-agency gateways
	Web Page Development	DC Superior Court web Page
	Secure Firewalls	To limit access to authorized users
	Criminal Information System	Criminal Record maintenance system
	Juvenile Information System (JISRA)	1981-98 Juvenile records
	Transaction Data Management System (TDM)	Civil data maintenance system
	Domestic Relations Systems	Domestic relation case record system

AGENCY	SYSTEM NAME	DESCRIPTION
	Jury Information System	Jury process application system
	Court Reporter Information System (CRP)	Contains court reporter data information
	Probate Data Information System (PRO)	Contains probate case information
	Personal Data System	Personal data record maintenance system
	Child Support Enforcement and Collections	N.O.I, IRS Intercept, wage attachment
	Courtwide caseload Management system	To replace current systems
	OPAL Middleware	Domestic Violence In-Take
	Juvenile Drug Court	To integrate JISRA/DTMS(PRISM)
	Legacy Systems	To make systems Y2K compliant
United States Attorney's Office	Network	USAO network with multiple servers, 486 and Pentium
	Replicated Criminal Information System (RCIS)	Imports CJIS, CIS data on daily basis into Oracle database
	Victim witness automated Transaction Statistics (VWATS)	Capture victim data at the time of intake
	Search warrant automated Transaction Statistics (SWATS)	Tracks search warrants issued in specific public addresses
	Personal Transaction Statistics (PTS)	Tracks personal, administrative information on employee
	Legal Information office network system(LIONS)	Tracks federal criminal and civil investigations and cases
Youth Services Administration	Adolescent Transaction Statistics (ACTS)	Maintains client records of basic, personal, family information
	Mini – Computer	IBM AS/400 mini computer that houses the ACTS

4.4 Operations Summary

The previous section gave a high level view of the IT infrastructure of all of the JUSTIS agencies. This section focuses on the CJCC selected initial contributors to the proof-of-concept – Metropolitan Police Department and Court Services and Offender Supervision Agency. This section offers further detail of the legacy systems and their inter-agency system connections for these two agencies.

4.4.1 Metropolitan Police Department

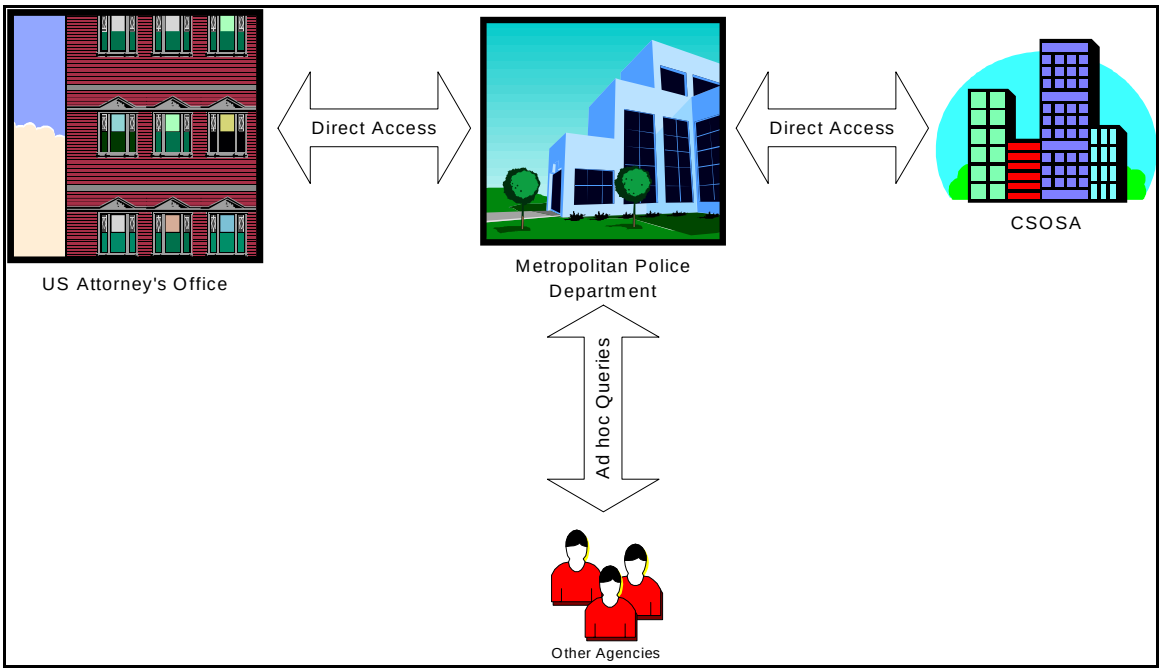


Figure 33 – Conceptual View of Current Data Exchanges From MPD

The Metropolitan Police Data (MPD) currently maintains two mission critical computer systems: the Washington Area Law Enforcement System (WALES) and the Criminal Justice Information System (CJIS), which together provide the primary support to the majority of the business processes within the Metropolitan Police Department. WALES and CJIS reside on an IBM mainframe.

The mission critical applications that reside in WALES are operated and maintained by the Metropolitan Police Department. CJIS is operated and maintained by the Pretrial Services.

WALES is utilized by the Metropolitan Police Department and other law enforcement agencies for investigative, criminal warrant, registration and court activities.

The CJIS was designed to serve all agencies of the District's Criminal Justice community by providing an offender base system to monitor and track individuals through the criminal justice system and provide current information on-line regarding each offender. The Metropolitan Police Department serves as the largest source of information for CJIS.

The lack of integrated information systems cause unnecessary delays by requiring multiple logins to other functional areas of MPD for processing input (e.g., CJIS, WALES) which result in redundant, and labor-intensive work.

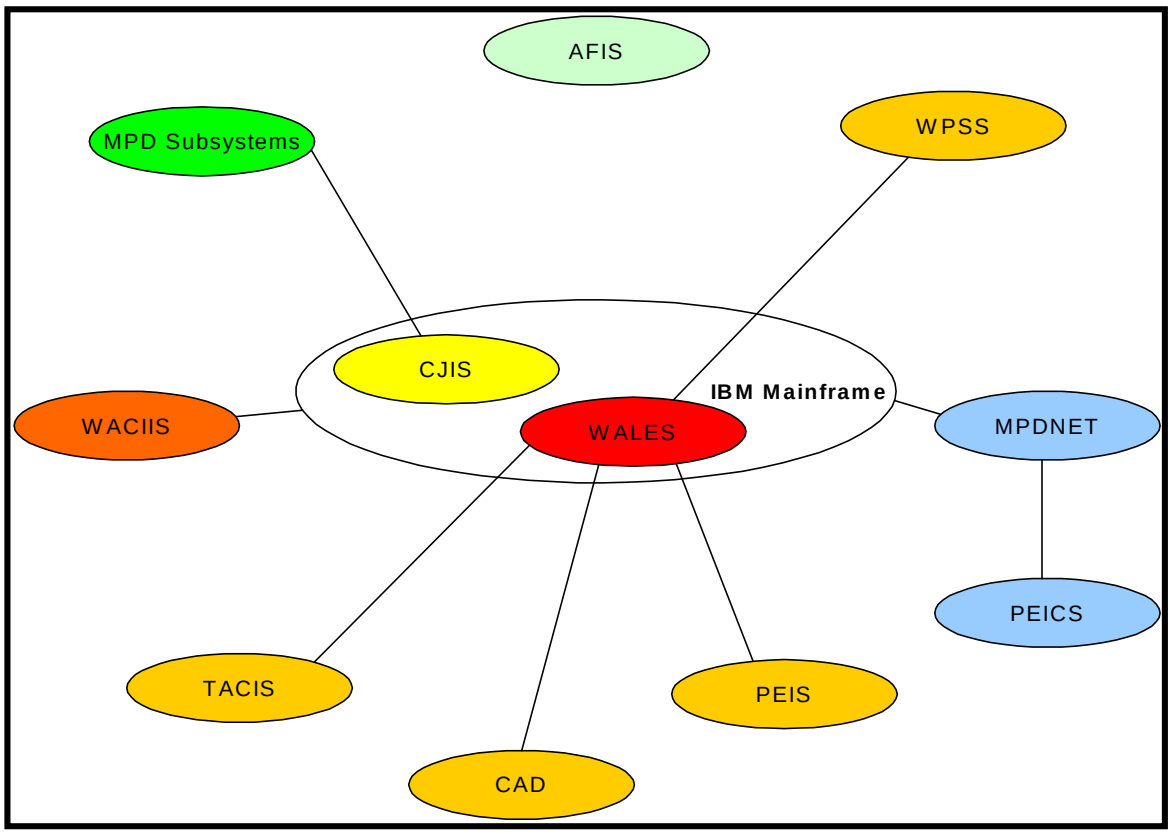


Figure 34 – Mission Critical MPD Legacy Applications

4.4.2 Pretrial Services Agency and Parole Agency

The Pretrial Services Agency and Parole Agency both maintain two mission critical systems.

The Pretrial Services Agency maintains a mainframe system named ABADABA (Automated Bail Agency Database). ABADABA contains arrested persons' pretrial data (e.g. charges, pretrial release status) in the mainframe file format known as VSAM. This data provides information pertaining to persons being arrested and processed through the District of Columbia's Court System. ABADABA is interfaced with the Metropolitan Police Department's WALES and is accessible to the MPD and other criminal justice agencies.[8]

The Parole Agency maintains a relational database information system called PARIS (Parole Information System). PARIS contains persons' pertinent parole information (e.g. parole length, parole violation).

[8] Perot Systems Corporation, "Business Engineering "As-Is" Process Document for MPD Operational Process." October 27, 1995

PARIS delivers information to the Metropolitan Police Department's CJIS information system via periodical batch processing.

4.5 User Workstations

The table below contains a summary of the current workstations at each of the justice agencies in the District of Columbia.

Agency User Workstation Summary

Agency	Desktop Platforms	Operating System	Internet Browser	Internet Access	Virus Protection
Corporation Council	350 – 300Mhz, PIII, 64 MB RAM 6GB HDD	350 – Windows NT	350 – IE, 5 - Netscape 4.0	20	McAfee 4.0.7
C.S.O.S.A	550Mhz PIII 128 MB RAM 8GB HDD ~800	Windows 98 ~750, NT4.0 ~50	IE ~800	~800	Norton AV ~800
DC Department of Correction	550Mhz PIII 128 MB RAM 12G HDD ~130	NT 4.0	IE5.0	35	McAfee 4.0.2
	500Mhz PIII 128MB RAM 10GB HDD ~50	NT 4.0	IE 5.0	40	McAfee 4.0.2
	450Mhz Pentium III 128 MB RAM, 10 GB HDD ~25	NT 4.0	IE 5.0	25	McAfee 4.0.2
	Pentium II 400Mhz 128MB RAM 2GBHDD ~150	Windows 95	IE 5.0	10	McAfee 4.02
	266Mhz Pentium 64MB RAM 2GB HDD ~150	Windows 95	IE 5.0	50	McAfee 4.02
	133Mhz Pentium 16MB RAM 2GB HDD ~130	Windows 95	IE 5.0	65	McAfee 4.02
DC Superior Court	233–300Mhz 32-64 MB RAM 1.3 GB HDD ~500	W95/98 ~500	IE5.0 ~100	~100	Norton
Metropolitan Police Department	450Mhz PII 126MB 6GB ~1000	NT 4.0	Netscape	~1000	Norton
	450Mhz PII 126MB 6GB ~1000	NT 4.0	Netscape	~1000	Norton
	4500Mhz PII 128MB 9GB ~400	NT4.0	IE4.0	~400	Norton
	166-233Mhz 32-64MB 2GB ~350	NT4.0 W95/98	Netscape	~350	Norton
	266Mhz 64 MB 6GB ~100	NT4.0 W95/98	Netscape	~100	Norton

Agency	Desktop Platforms	Operating System	Internet Browser	Internet Access	Virus Protection
Public Defender	Micron Pent II 350Mhz 64 MB RAM 24XCD ROM 8GHD 3Com 10/100 NIC ~150	WidowsNT~50 Win 95 ~100	IE5.0 ~205	~205	Scan Mail for exchange server ~1 & Inoculate IT V4.53 Server & Workstation ~250
	Micron Pent III 400Mhz 64 MB RAM 8GHD 3Com 10/100 NIC ~40	Win 95	IE 5.0	40	Inoculate IT V4.53 Server & Workstation
	HP Vectra P100 24 MB RAM 2.5GHD 3Com 10/100 NIC ~15	Win 95	IE 5.0	15	Inoculate IT V4.53 Server & Workstation
US Attorney	366 MHZ Pentium 128 MB ~ 800	WinNT ~800	Netscape 4.7	~800	Inoculan 4.0 for NT ~800
US Parole Commission					
Youth Services Administration	350 Mhz PentIII 128 MB RAM ~115	Win NT ~115	IE5.0	~115	VirusScan 4.0

4.6 Summary

The information presented above provides a summary of the current IT environments within the justice agencies. This information will be compared with the IT infrastructure requirements set forth in the Future Systems section of the JUSTIS Blueprint. This comparison generates a list of “gap” points that are laid out in the next section of the document. These “gap” points provide the basis for the development of the roadmap, which will present a logical process for a multi-phased implementation of the JUSTIS System.

5. Roadmap

5.1 Introduction

This Blueprint document began with a definition of the system's mission and business requirements. It then moved on to a description of the complete vision for the future JUSTIS System once it has been fully developed and implemented. Those sections collectively define the end-state goal.

The preceding section summarized the elements of the current environment. That section defined the point from which the JUSTIS System and its community of users must start towards the eventual end-state goal.

This section presents an analysis of the gap areas between where we are and where we want to be. Once these gap areas are identified, organized and prioritized, a roadmap is presented. This roadmap shows a number of steps towards the full implementation. The following diagram depicts how we have proceeded through this document, and we are now in the final steps:

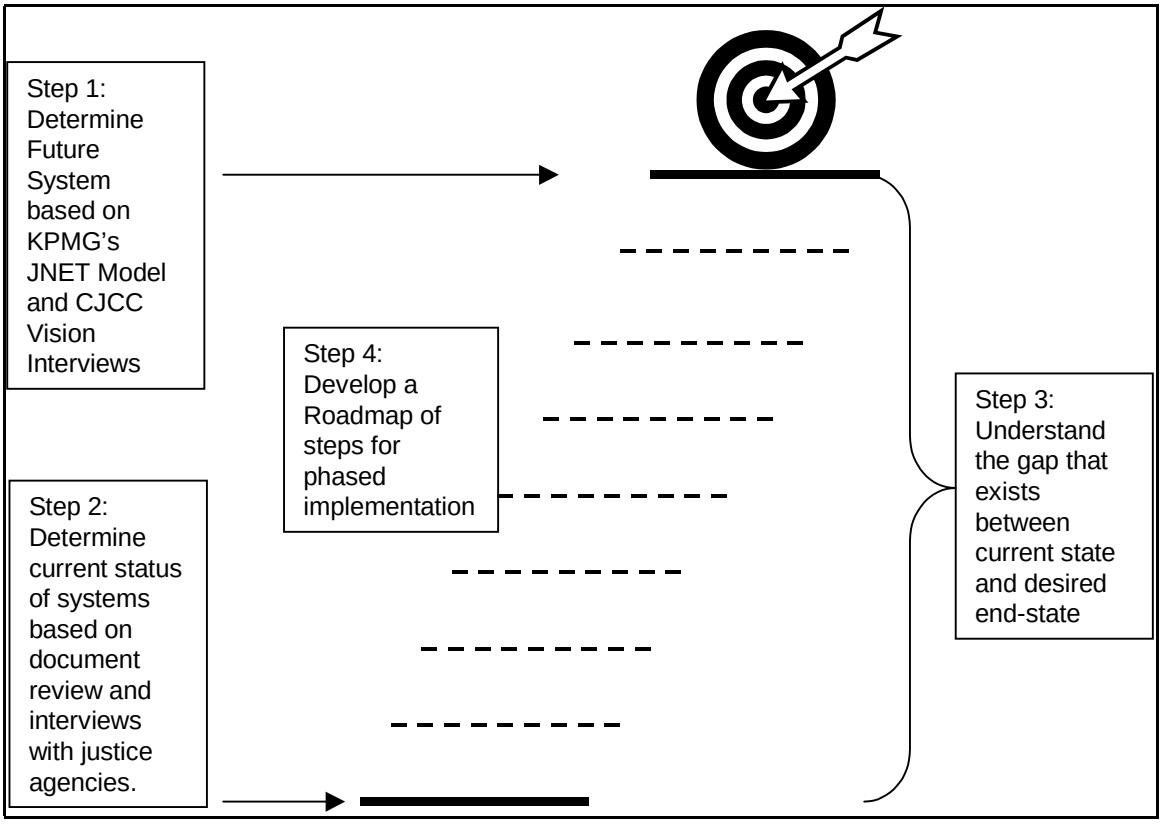


Figure 35 – Blueprint Format

JUSTIS will be implemented in phases. This allows the justice user community to realize short-term gains while proceeding toward the entire vision. Multi-phase implementation also allows the system to keep in

time with contemporary technologies throughout the implementation. The roadmap defines the phased implementation.

5.2 Identification of Gap Areas

The variance between current environment capabilities vis-à-vis the environment necessary to support the full JUSTIS System is analyzed in this section. JUSTIS is a new system for the District. Therefore, the gap is substantial. The gap has been partially closed by the proof-of-concept phase.

5.2.1 Gap Areas for the Functional Requirements

5.2.1.1 Agency Participation and Information Sharing Modes

During the proof-of-concept phase, two agencies are participating by contributing their data. These are the Metropolitan Police Department and Court Services and Offender Supervision Agency. Additionally, five agencies are participating with three users each to evaluate the proof-of-concept system.

The gap therefore is to increase agency data contributors and agency system users. The list of potential agencies comes initially from membership in the CJCC. In the future, other agencies such as the Department of Motor Vehicles could also play an important role within the JUSTIS System.

5.2.1.2 Secure Email

JUSTIS agency participants are currently not running email systems with the level of full security defined by JUSTIS. Additionally, there are multiple, disparate email systems in use amongst the CJCC represented agencies. For example, Lotus Notes, Microsoft Exchange, Lout cc:Mail and IBM PROFS are all in use.

The proof-of-concept system does not include secure email as a component. The gap therefore is two-fold. First, a separate email system for JUSTIS is to be implemented. This email system will use the SMTP, POP3/IMAP4, LDAP, and security mechanisms of the JUSTIS Hub servers. Under this scenario, JUSTIS users would have two email systems to use: the one they normally use within their agency and the JUSTIS secure email system.

The second mechanism for secure email would take place if the CJCC participating agencies selected and implemented a common email platform with the security capabilities of the JUSTIS architecture. This would enable JUSTIS users to use only one email system for all of their electronic mail activities.

5.2.1.3 Notification Services: Publish and Subscribe

Under the POC, notification services are not yet implemented. The gap here is to conduct a detailed analysis of the feasibility and functionality for a notification service and to design and implement this functionality into JUSTIS.

Notification services could be on an individual basis or a group basis. For example, when a parolee is arrested and booked, this event (the police booking) can generate a notification to either a single, subscribed parole officer or the entire Parole agency.

The decision on whether to perform notifications on a group basis or individual basis is one that will need to be addressed by the ITAC during final Blueprint preparations. The decision will be driven by a cost

benefit analysis. Individual notifications demand a greater level of system sophistication as well as higher demands for administration and operation of the system. In the end, phased implementation may determine to start with group notification and move towards individual notification in a later phase. Knowing this in advance will affect the design of each phase of implementation.

5.2.1.4 Collaborative Services: Discussion Groups

Discussion groups are not yet part of the JUSTIS System. The gap is to define the requirements of the system, select and purchase software that meets the requirements, implement the software and finally implement the discussion groups and their administration.

5.2.1.5 Data Transfer

Data transfer is not currently performed as part of the JUSTIS POC. To close this gap, the project team will need to identify likely areas for data exchange, analyze mechanisms already in place to enable limited data exchange (such as file transfers or manual disk exchange) and work with the participating agencies to design programs and procedures to enable JUSTIS System data transfer.

5.2.1.6 Data Cleansing Notification and Processes

Data cleansing and notification processes are not part of the JUSTIS POC. This gap can be closed by:

- Determining participating agency data administrators. These are the staff that will correct their source data once they have been notified of a problem.
- Designing the inquiry application screens to contain a button that sends a copy of the data page in question, along with the sender's comments, to the data administrator.
- Designing and implementing the security mechanisms to allow for secure transmission of the error reports. These reports may be sent via secure email or may be posted to a discussion group.
- Designing and implementing an auditing mechanism to ensure that the person making a data cleanliness report and the data administrator responsible for the action have reached an agreement on the issues closure.

5.2.1.7 Offender Contact Points

The creation of the offender contact points after the JUSTIS POC would involve the coding of a special set of query programs that collected the contact from each agency and summarized the results on a single page.

5.2.1.8 Public Access

The largest considerations for public access to JUSTIS data are for the CJCC to determine which data is to be shared and for the ITAC, JUSTIS System Manager and Security Officer to determine the separate hardware, software and security infrastructure necessary to isolate the publicly accessible data from the private JUSTIS System.

5.2.1.9 Database for Statistical Analysis

As was stated in section 3.3.8 Database for Statistical Analysis, many of the components for a statistical analysis database will be in place once JUSTIS is fully operational. Nevertheless, there are significant infrastructure components necessary for a full deployment. The following diagram shows the nature of these hardware and software elements.

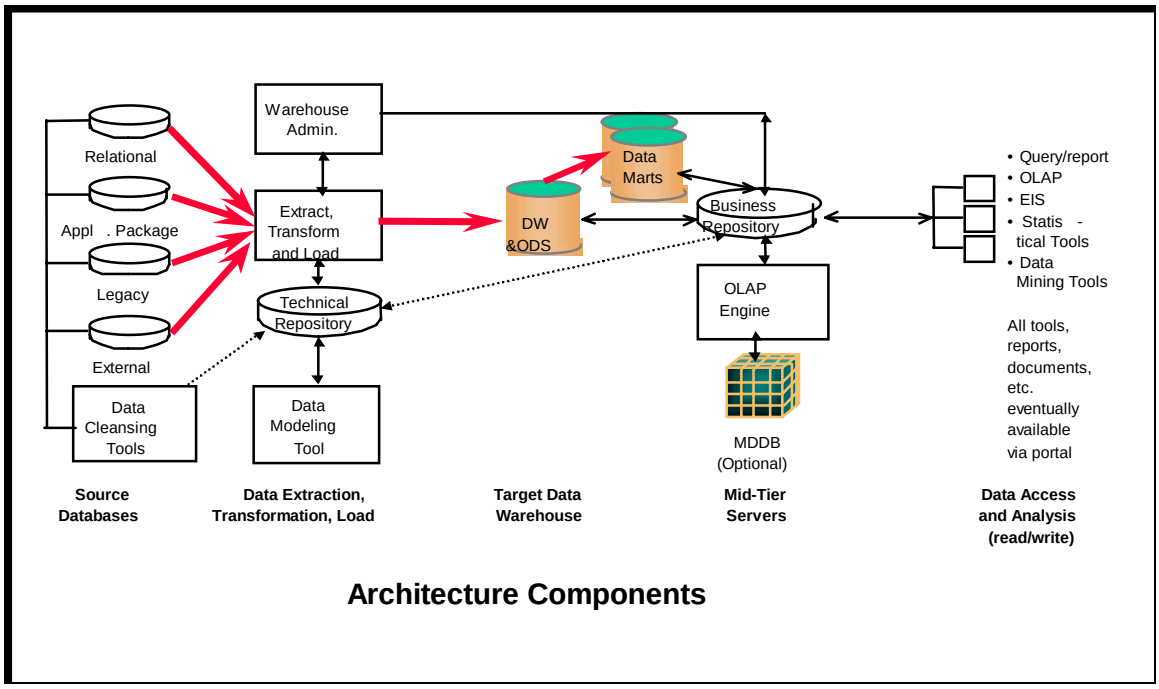


Figure 36 - OBTS Architecture Components

This diagram shows that at least the following software elements need to be considered for the OBTS:

TYPE OF TOOLS	MARKETPLACE EXAMPLES
Data Cleansing Tools	Evoke, Vality
Address Cleansing	Code/1
Extract/Transform/Load	Carleton PureView
Main DW and ODS	Oracle, IBM UDB on Sun Solaris
Data Marts	SQL Server on NT platform
Query/Reporting	Business Objects Web Intelligence
OLAP	Cognos
Statistical Tools	SAS
Data Mining	SAS; Business Objects Business Miner
Portal Technology	IA Eureka; Sequoia
Agents/Alerts	Netview; Unicenter

5.2.2 Gap Areas for the Technical Architecture

The gap areas between the current technical architecture and the architecture necessary to support JUSTIS are as follows:

- **Full security implementation**. The document developed by Mitretek and attached in the appendix of the Blueprint defines the security policies and procedures with regards to a full security implementation. It is recommended that an initial step in the full security implementation is to develop a security implementation strategy based upon the requirements defined in the Mitretek document. A logical first step is the implementation of a certificate server, a directory server to store the certificates, and an S/MIME capable email system.

- **JUSTIS building blocks**. The use of open standards and J2EE will continue with JUSTIS. New releases in the standards will require evaluation for possible JUSTIS upgrade.

- **Physical Plant Design.** The JUSTIS POC has begun with a physical plant design that will be compatible with the final version of JUSTIS. The District will need to evaluate machine room locations for JUSTIS expansion. A disaster recovery plan should be developed that addresses such items as redundant servers and network connections.

- **Scalability and Performance Requirements.** The JUSTIS POC is built on production-quality servers and should maintain good performance through a growing number of users. The full JUSTIS System should include performance monitoring and reporting tools. The performance should be monitored by the JUSTIS operations staff, and a pro-active plan for addressing performance concerns should be developed well in advance of need. This plan should include guidelines for upgrading server hardware (number of and speed of CPU's, memory and disk components) and for implementing load balancers to spread the transaction load across multiple servers.

- **User workstations.** All user workstations should be able to run a modern web browser such as Microsoft Internet Explorer or Netscape. JUSTIS participating agencies should review their user workstations in relation to this requirement. Older terminals, such as IBM 3270 devices, should be scheduled for upgrade.

- **Network Infrastructure: special security requirements.** The Mitretek security requirements document contains the relevant information on security requirements. This document details management control requirements, operational controls, and technical controls. Further security analysis remains to be done to determine items such as required firewall devices and the devices' configuration.

- **Application Development Guidelines.** This Blueprint has suggested some application development guidelines for JUSTIS participating agencies to follow in order to maintain compatibility with the system. The JUSTIS office should implement a mechanism to assist participants in sharing their plans and assisting one another in their system upgrade strategy development.

- **Off-line, Replicated and On-line Data**. As agencies are added to the JUSTIS community, each will need to decide the strategy for making their data available to the participants. As a part of this, a database administrator should be identified and assigned early in the decision process.

5.2.3 Gap Areas for Management and Administrative Structure

The future administrative and management structure for JUSTIS was defined as follows:

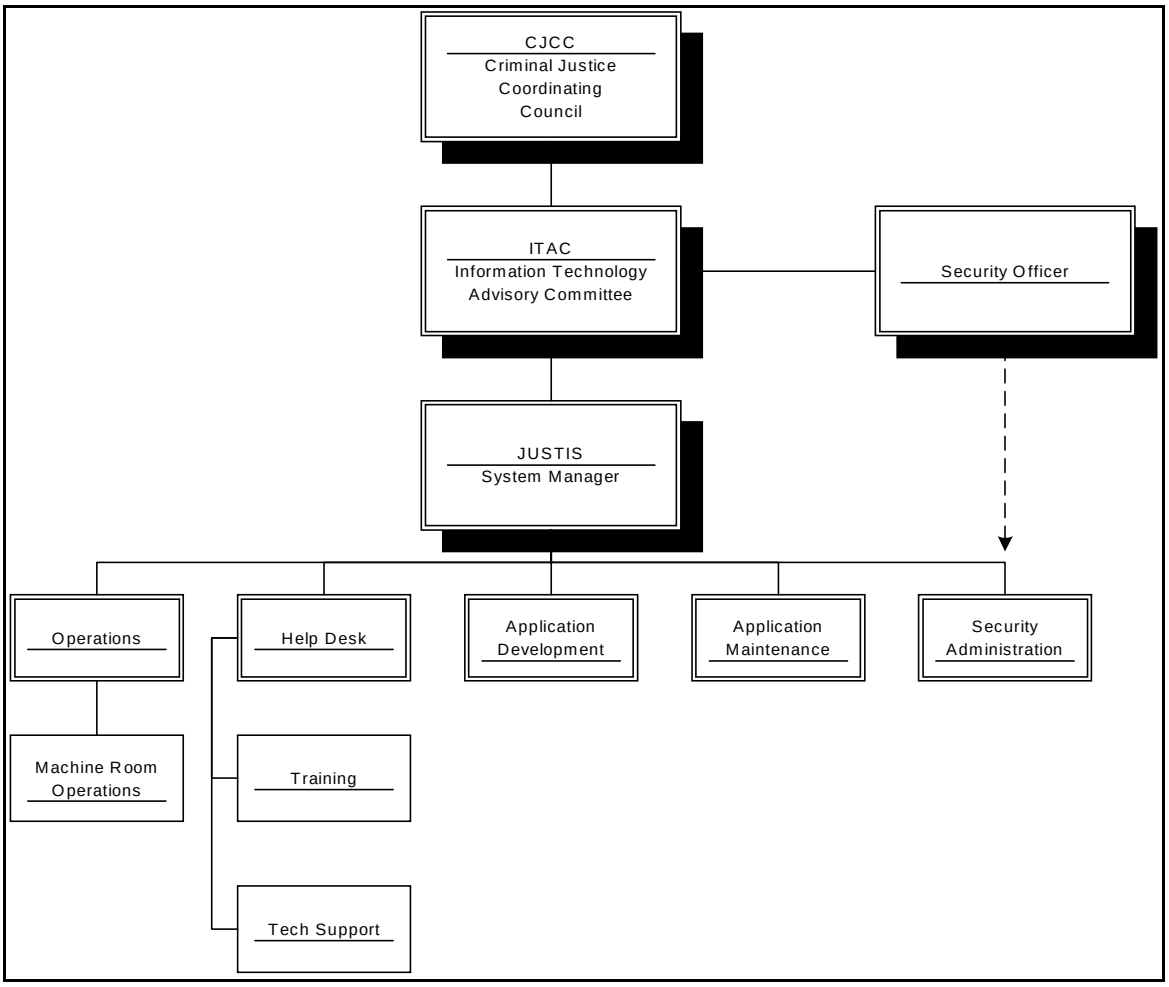


Figure 37 – Future JUSTIS Administrative and Management Structure

The JUSTIS System is being implemented in phases, and the JUSTIS office structure will also be implemented in phases. During the proof-of-concept phase, the JUSTIS team is organized as follows:

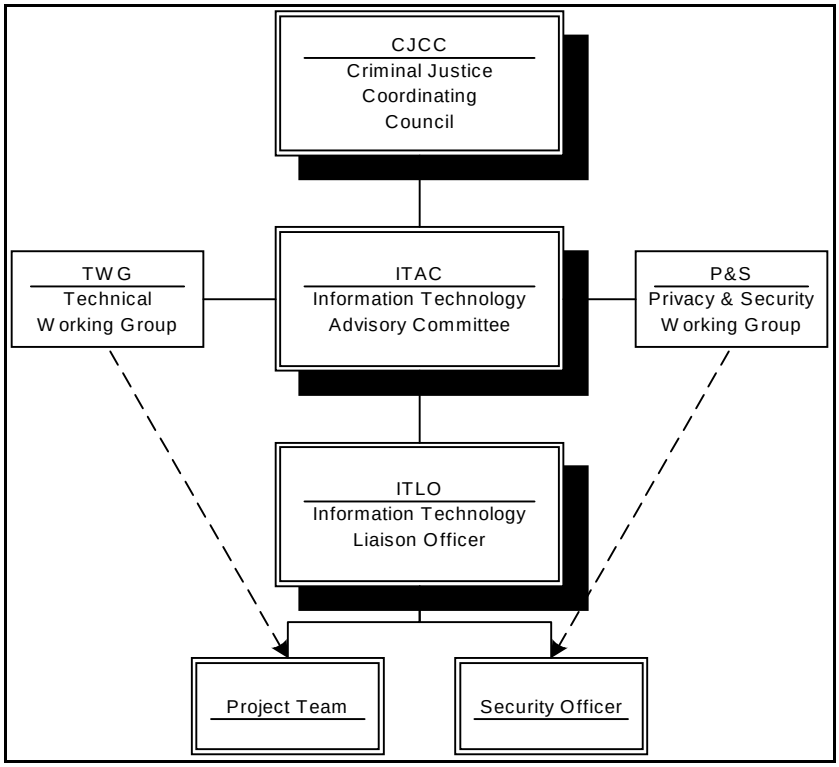


Figure 38 – POC JUSTIS Administrative and Management Structure

In this proof-of-concept structure, the project team is from KPMG and is performing a subset of the duties that will ultimately be spread across Operations, Help Desk, Applications Development and Application Maintenance. The project team is receiving guidance from the Technical Working Group during POC development. The project team is being managed by the ITLO.

CJCC staff is fulfilling the Security Officer role with supplemental assistance from Mitretek. The security team is receiving guidance from the Privacy and Security Working Group during POC development.

Once the POC has been developed and deployed, the JUSTIS office structure will change again to accommodate an environment where the initial system needs support at the same time that new system functionality is being developed. This transition structure is depicted in the following diagram:

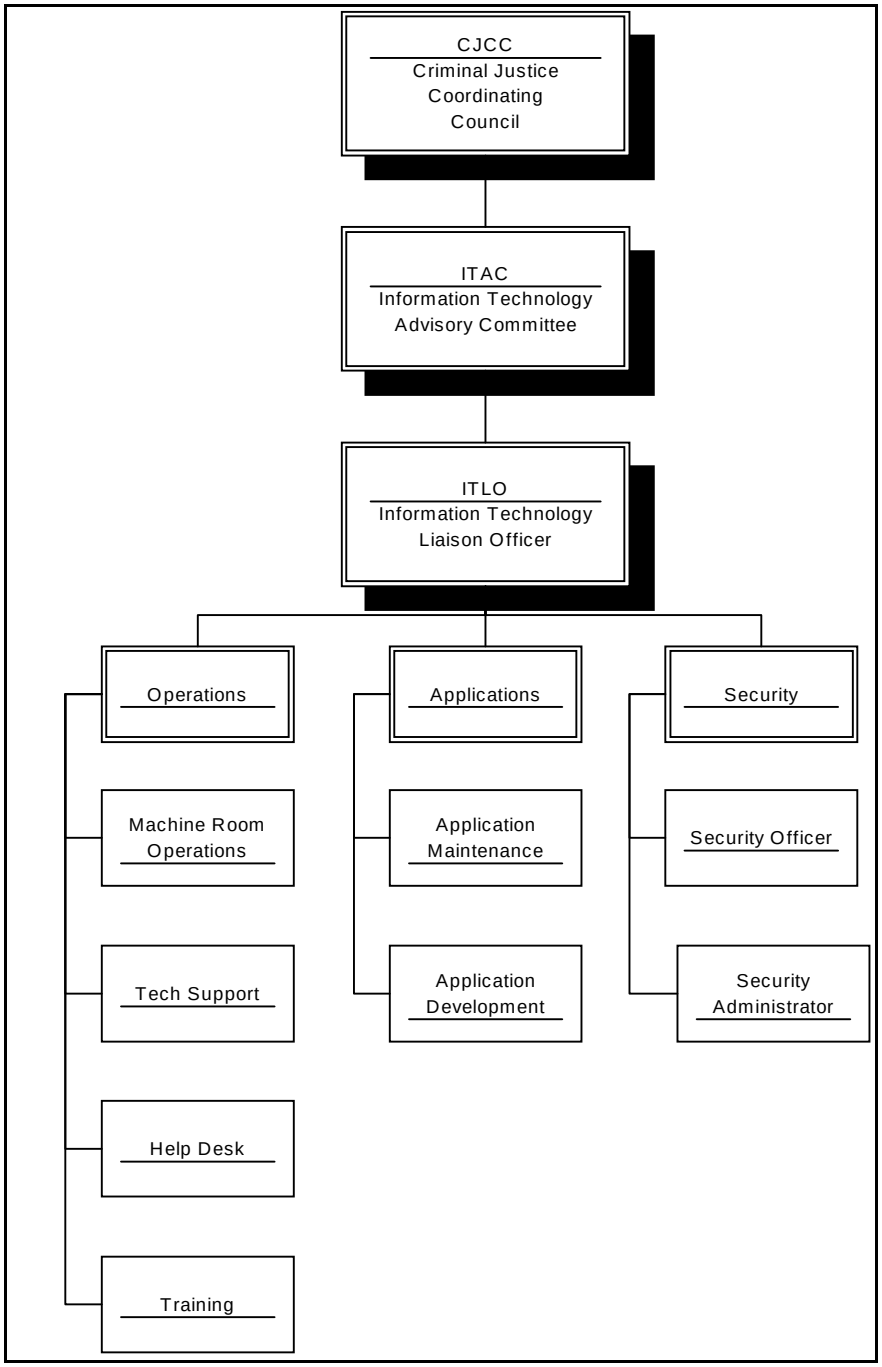


Figure 39 – Interim JUSTIS Administrative and Management Structure

The above diagram depicts a separation of departmental roles and each staff box does not necessarily represent a single staff member. During this transition stage, some staff overlap will likely occur. For example, in the help desk department, a single staff member may handle training and technical support. During this phase, applications maintenance will likely be a responsibility of the application development staff.

Once in production, management of the system is the leading contributor to the system's effectiveness. The complexity of the relationships of the justice agencies in the District of Columbia necessitates an independent management and administrative office for the JUSTIS System. A major function of this office is to formulate the correct rules of publication and access to criminal justice data.

5.3 Summary and Prioritization Ranking of Gap Areas

The gap areas identified in the preceding section are organized in the table below. The organization is based in priority of implementation as well as interdependencies. An example of interdependency is that a security certificate server and infrastructure are necessary before secure electronic mail can be implemented. For completeness, the proof-of-concept statement of work tasks are shown.

Summary and Prioritization Ranking of Gap Areas	
Create A JUSTIS Proof-Of-Concept	
	Perform initial review of existing DC produced work products.
	Identify and assign District "core" team members and justice agency representatives.
	Refine all project tasks as necessary.
	Finalize proof-of-concept project plan as required.
	Institute project record keeping and accounting procedures.
	Develop regular status meeting schedule.
	Establish project level communications plan, including CJCC, OCTO, ITAC and its sub-groups (e.g., Analysis and Design, Technical Work Group).
	Prepare proof-of-concept kick-off presentation materials.
	Conduct proof-of-concept kick-off meeting.
	Develop a Blueprint outline.
	Obtain approval of Blueprint outline.
	Obtain current technical architecture inputs from participating agencies (e.g., hardware/software inventories, architecture diagrams).
	Develop Blueprint working draft content.
	Conduct Blueprint walkthrough.
	Prepare Blueprint for distribution.
	Update Blueprint working draft.
	Distribute final Blueprint.
	Develop mock-up of a proposed framework.
	Obtain input from participating agencies for static content.
	Develop agency-specific static content.
	Develop general static content.
	Test web site components and links.
	Work with participating agencies to determine data to be published.
	Design screen formats.
	Design programs to access agency databases.
	Develop programs to access agency databases.
	Perform testing.
	Deploy application
	Develop requirements for the development environment.
	Support the acquisition of hardware/software/network components for the development environment.

Summary and Prioritization Ranking of Gap Areas	
	Support the set-up of the development environment.
	Develop requirements for the test environment.
	Support the acquisition of hardware/software/network components for the test environment.
	Support the set-up of the test environment.
	Development requirements for production environment.
	Support the acquisition of hardware/software/network components for the production environment.
	Support the set-up of the production environment.
	Document development, test, and production environments
	Review adequacy of user workstations.
	Identify any needed upgrades.
	Prepare user workstations for implementation.
	Deploy browser and other appropriate software on three (3) workstations within five (5) agencies.
	Provide up to three (3) half-day training sessions to designated users or trainers.
	Deploy application to three (3) workstations within five (5) agencies.
	Document standard workstation configuration
Create a production environment for JUSTIS	
	Install production firewalls and other security hardware
	Install Discussion Group Software
	Install Certificate Authority server
	Implement security policies and procedures for JUSTIS users
	Implement system monitoring facilities
	Purchase Certificates for all users and servers
	Develop disaster recovery plan
	Add LDAP Server to Hub environment
	Develop operations procedures (backup/restore, preventive maintenance)
	Develop help desk materials – frequently asked questions, user manual
	Hire, contract operations staff
	Hire, contract applications development and maintenance staff
	Hire, contract help desk staff
	Install SMTP/POP3 mail server
Increase Data Contribution	
	Superior Court of DC Data Contribution
	DC Department of Corrections Data Contribution
	Federal Bureau of Prisons Data Contribution
	US Parole Commission Data Contribution
	US Attorneys Office Data Contribution
	Youth Services Administration Data Contribution
	Office of Corporation Counsel Data Contribution
	Add DMV information – driver's licenses, photos
Prepare JUSTIS Agency Environment	
	Superior Court of DC JUSTIS Server hardware and software
	DC Department of Corrections JUSTIS Server hardware and software
	Federal Bureau of Prisons JUSTIS Server hardware and software

Summary and Prioritization Ranking of Gap Areas	
	US Parole Commission JUSTIS Server hardware and software
	US Attorneys Office JUSTIS Server hardware and software
	Youth Services Administration JUSTIS Server hardware and software
	Office of Corporation Counsel JUSTIS Server hardware and software
	DC Department of Corrections provide static web content
	Federal Bureau of Prisons provide static web content
	US Parole Commission provide static web content
	US Attorneys Office provide static web content
	Youth Services Administration provide static web content
	Office of Corporation Counsel provide static web content
Prepare JUSTIS Users	
	Superior Court of DC – identify JUSTIS users
	DC Department of Corrections – identify JUSTIS users
	Federal Bureau of Prisons – identify JUSTIS users
	US Parole Commission – identify JUSTIS users
	US Attorneys Office – identify JUSTIS users
	Youth Services Administration – identify JUSTIS users
	Office of Corporation Counsel – identify JUSTIS users
	Superior Court of DC – prepare user workstations
	DC Department of Corrections – prepare user workstations
	Federal Bureau of Prisons – prepare user workstations
	US Parole Commission – prepare user workstations
	US Attorneys Office – prepare user workstations
	Youth Services Administration – prepare user workstations
	Office of Corporation Counsel – prepare user workstations
Increase JUSTIS System Functionality	
	Implement secure email capability for test group of users
	Implement secure email capability for all users
	Setup discussion groups (e.g. assign moderator)
	Implement underlying messaging structure for notification
	Implement publish/subscribe event notification at group level
	Implement publish/subscribe event notification at individual level
	Enhance notification – add email, pager, voice alerts
	Implement infrastructure for statistical database
	Populate a statistical analysis database
	Develop statistical analysis queries
	Implement a separate system for controlled public access
	Analyze agencies for data transfer implementation needs
	Design interagency data transfer programs and procedures
	Test data transfer capabilities
	Fully implement and support data transfer

5.4 Proposed Phases of Implementation

Now that the gap items have been prioritized and analyzed for interdependencies, the gap items will be partitioned into phases for future release implementations of the JUSTIS System. In addition to priority and interdependence, phase steps have been chosen for their simplicity of implementation relative to the value they provide. This means that early phases will combine items necessary for infrastructure support as well as items that return high value for a relatively small investment.

5.4.1 Phase 1 – POC

The POC solution has been defined and accepted in the original JUSTIS statement of work and the project plan approved by the ITAC on July 20, 2000. The POC demonstrates that it makes progress towards the future state by closing a number of gap items. The POC is the first step in a phased implementation of the full JUSTIS System. Future phases will expand upon the core functionality initially deployed in the POC.

5.4.2 Phase 2 – From POC to Production

Once the POC has been evaluated and the decision has been made to move forward with a more complete JUSTIS implementation, the next step is to make the POC system a production system within DC. For example, this phase will require the implementation of a security office, an operational staff, and a help desk and training center. These operational centers may be organized under a JUSTIS administrative office.

Phase 2 Tasks	
Create a production environment for JUSTIS	
	Install production firewalls and other security hardware
	Install Discussion Group Software
	Install Certificate Authority server
	Implement security policies and procedures for JUSTIS users
	Implement system monitoring facilities
	Purchase Certificates for all users and servers
	Develop disaster recovery plan
	Add LDAP Server to Hub environment
	Develop operations procedures (backup/restore, preventive maintenance)
	Develop help desk materials – frequently asked questions, user manual
	Hire, contract operations staff
	Hire, contract applications development and maintenance staff
	Hire, contract help desk staff
	Install SMTP/POP3 mail server

5.4.3 Phase 3 – Increase Users and Add Secure E-Mail and Discussion Groups

This phase includes increasing the numbers of users, both within the POC participating agencies as well as with new agencies. In addition, the introduction of collaborative newsgroups in this phase returns high value with a relatively small investment. Secure email is implemented to take immediate advantage of the security infrastructure put in place during the previous phase.

Phase 3 Tasks	
Prepare JUSTIS Users	
	Superior Court of DC – identify JUSTIS users
	DC Department of Corrections – identify JUSTIS users
	Federal Bureau of Prisons – identify JUSTIS users
	US Parole Commission – identify JUSTIS users
	US Attorneys Office – identify JUSTIS users
	Youth Services Administration – identify JUSTIS users
	Office of Corporation Counsel – identify JUSTIS users
	Superior Court of DC – prepare user workstations
	DC Department of Corrections – prepare user workstations
	Federal Bureau of Prisons – prepare user workstations
	US Parole Commission – prepare user workstations
	US Attorneys Office – prepare user workstations
	Youth Services Administration – prepare user workstations
	Office of Corporation Counsel – prepare user workstations
Increase JUSTIS System Functionality	
	Implement secure email capability for test group of users
	Implement secure email capability for all users
	Setup discussion groups (e.g. assign moderator)

5.4.4 Phase 4 – Increasing Data Contribution

This phase includes increasing the number of contributing agencies. This involves the development of additional inquiry applications as well as the static content for the agencies to fit within the framework.

Phase 4 Tasks	
Increase Data Contribution	
	Superior Court of DC Data Contribution
	DC Department of Corrections Data Contribution
	Federal Bureau of Prisons Data Contribution
	US Parole Commission Data Contribution
	US Attorneys Office Data Contribution
	Youth Services Administration Data Contribution
	Office of Corporation Counsel Data Contribution
	Add DMV information – driver's licenses, photos
Prepare JUSTIS Agency Environment	
	Superior Court of DC JUSTIS Server hardware and software
	DC Department of Corrections JUSTIS Server hardware and software
	Federal Bureau of Prisons JUSTIS Server hardware and software
	US Parole Commission JUSTIS Server hardware and software

Phase 4 Tasks	
	US Attorneys Office JUSTIS Server hardware and software
	Youth Services Administration JUSTIS Server hardware and software
	Office of Corporation Counsel JUSTIS Server hardware and software
	DC Department of Corrections provide static web content
	Federal Bureau of Prisons provide static web content
	US Parole Commission provide static web content
	US Attorneys Office provide static web content
	Youth Services Administration provide static web content
	Office of Corporation Counsel provide static web content

5.4.5 Phase 5 – Notification Services

Phase 5 includes increasing the functionality of the JUSTIS System with publish and subscribe event notification.

Phase 5	
Increase JUSTIS System Functionality	
	Implement underlying messaging structure for notification
	Implement publish/subscribe event notification at group level
	Implement publish/subscribe event notification at individual level
	Enhance notification – add email, pager, voice alerts

5.4.6 Phase 6 – Data Transfer

Phase 6 might include the ability for data transfer. For example, a person is arrested and a new arrest record is created. When that person comes up for trial, the JUSTIS System could assist the court in importing the arrest record information into a new case record. If the outcome of the case results in probation, then the JUSTIS System could support the probation office importation of the same intake data.

Phase 6 Tasks	
Increase JUSTIS System Functionality	
	Analyze agencies for data transfer implementation needs
	Design interagency data transfer programs and procedures
	Test data transfer capabilities
	Fully implement and support data transfer

5.4.7 Phase 7 – Public Access and OBTS

As the system evolves and the technology base upon which it is built expands, new enhancements become practical to implement. For example, certain data may be made publicly available. Another item to consider is using JUSTIS to populate a system with aggregated data for statistical analysis.

Phase 7 Tasks	
Increase JUSTIS System Functionality	
	Implement secure email capability for test group of users
	Implement secure email capability for all users
	Setup discussion groups (e.g. assign moderator)
	Implement underlying messaging structure for notification
	Implement publish/subscribe event notification at group level
	Implement publish/subscribe event notification at individual level
	Enhance notification – add email, pager, voice alerts
	Implement infrastructure for statistical database
	Populate a statistical analysis database
	Develop statistical analysis queries
	Implement a separate system for controlled public access

6. Conclusion

6.1 JUSTIS Proof of Concept

The JUSTIS Proof of Concept as defined in the original statement of work is the first step in a phased implementation of the full JUSTIS System and is to provide the initial functionality of limited data sharing through the use of an inquiry application. This has been accomplished by coordinating with three JUSTIS agencies (MPD, PSA, and CSOSA) and hosting the system through the District of Columbia's Wide Area Network. The hardware and software configuration of the JUSTIS System is outlined in appendix to this document. The development team has worked over the past six months developing, implementing and coordinating this effort. The POC is operational with functionalities that exceed the requirements.

6.2 Blueprint Architecture

The JUSTIS Blueprint is the foundation document of the JUSTIS System. This document was produced with the intention of describing and detailing the development of a solution that will serve the data sharing and collaboration needs of the CJCC participating agencies. The JUSTIS System is to become the backbone system servicing these needs. The JUSTIS Blueprint addresses the development of this System by focusing on the following critical implementation points:

- **The JUSTIS Business Requirements and Goals.** These requirements and goals were developed and managed by the CJCC for the benefit of the justice community of the District of Columbia and are to be used as a continual reference points throughout the development of the JUSTIS System. They are to become the guidelines in the development of a Public Safety Community of Interest (COIN) within the District of Columbia and are dynamic enough to change as the COIN's environment changes.

- **The JUSTIS System Implementation Strategy.** Implementation strategy is key in the development of highly technical information system. The JUSTIS System is designed with a multi-phased implementation strategy. This strategy provides advantages over a large, full-scale implementation. Short-term successes or quick wins are realized in an implementation strategy of this sort. Also, strategies such as this allow for the integration of current technologies throughout the implementation. Most importantly, a multi-phased implementation strategy provides time for validation of the long-term plan after each implementation phase.

- **The Future JUSTIS User Community and System.** The JUSTIS user community is made up of public safety agencies with the need for various elements of criminal justice data. These agencies also hold stores of criminal justice data that if transported securely, could be shared with other public safety agencies. The future JUSTIS System is designed to become a conduit in public safety agency data sharing and is described in its agreed upon "to be" form at the time of publication. Interagency functionalities of the JUSTIS System are centered around the JUSTIS business requirements and goals and implemented using the current technologies to date that correspond with those requirements and goals. The implementation of the desired interagency functionalities demand the integration of various technical architecture requirements. The JUSTIS Systems technical architecture takes into account these architecture requirements and integrates them into one architecture that considers system security, scalability, user workstations, network infrastructure, and application development along with other related factors.

- **The JUSTIS Community Current Systems Summary.** Becoming aware of the information technology environments residing in the public safety agencies is important to the successful implementation of the JUSTIS System. A core functionality of the JUSTIS System is to allow for data sharing from a variety of legacy systems and agency collaboration. The knowledge of the legacy systems allows the implementation team to design strategies for data extraction, inquiry and presentation through the JUSTIS System. These activities require the analysis of current systems security infrastructure, network infrastructure, user workstations, and legacy applications and the data contained therein. Analysis of the current business processes that are rudimentary attempts to provide similar JUSTIS functionalities are also critical to the JUSTIS implementation team. This avoids reinvention of current processes and lends itself to the expansion of the POC to the future phases by taking advantage of current agency relationships. This requires less change management throughout the agencies than would implementations that employ new business processes and the development of new relationships.

- **The JUSTIS Roadmap.** Taking the JUSTIS System from concept to production requires an evaluation and comparison of the public safety agencies current systems versus the end solution architecture. Involved in this comparison is the identification of gap areas between the two states and the prioritization of those gap areas. Following the multi-phased implementation strategy these gap areas are prioritized based upon a logical technological progression. By considering the results of closing each gap area, the gap areas are turned into implementation phases. These phases are prioritized based upon the phases' business impact and execution ease providing a roadmap that will lead to the successful implementation of the JUSTIS System as described in the Blueprint. The first phase described in the roadmap is the JUSTIS Proof of Concept.

- **JUSTIS Administrative and Management Structure.** The need for a JUSTIS Administrative and Management Office is critical to the JUSTIS implementation strategy. A multi-phased implementation across various entities requires a centralized and focused management team. The Blueprint defines and proposed structure that will expand as the JUSTIS System expands and will ultimately be able to perform the following duties:

  - System Operations
  - Help Desk
  - Application Development
  - Application Maintenance
  - Security Management
  - Change Management

  It is important to realize that the Blueprint describes the conceptual administrative and management structure. During the implementation of the JUSTIS System the administrative and management structure will be developed in consideration of not only the conceptual design in the Blueprint but the security management control requirements as described in the document produced by Mitretek, as well as other relevant external factors.

The JUSTIS Blueprint is a deliverable that is defined in the first phase of implementation of the JUSTIS System. It is a result of the knowledge gained through analysis of the District of Columbia justice community and has been refined and validated through the implementation of the JUSTIS System Inquiry Application. It was compiled and written in consideration of CJCC requirements and constraints.

This document was first delivered in draft form on August 31, 2000. After the implementation of the JUSTIS POC, the Blueprint was updated to include the most relevant information. Items that have been either updated or added to the Blueprint since its draft form delivery are:

- **Mitretek Security Requirements** – The CJCC contracted with Mitretek to define and deliver the security requirements necessary for the full implementation of the JUSTIS System. This documents is titled the "District Of Columbia (DC) – Justice Information System (JUSTIS) Security Control Requirements", and is a separate document that is only referenced in the Blueprint.

- **Proof of Concept Hardware and Software Documentation** – The JUSTIS POC hardware and software configurations are outlined in a document titled "District of Columbia Government, Criminal Justice Coordinating Council, Hardware and Software Documentation for the JUSTIS Proof of Concept." This document is also attached in the appendices and is labeled Appendix A.

- **JUSTIS User Workstation Configuration** – The Blueprint Draft described the planned user workstation configuration for the JUSTIS System. This was described before the actual deployment of a functioning system. After the production of the JUSTIS POC the user workstation requirements were further detailed and are listed in section 3.4.5 of the final Blueprint.

- **JUSTIS Training Booklet** – Anticipating potential users with various technical skills, KPMG and the CJCC provided the opportunity for the initial users of the JUSTIS POC to participate in training. The JUSTIS POC Training consisted of a security requirements briefing, a demonstration of the POC, and a hands-on scavenger hunt exercise. KPMG provided the second part of the training. The training materials attached to the Blueprint were developed for and utilized in the second part of the JUSTIS POC Training. This document can be found in the appendices and is labeled Appendix B.

- **JUSTIS Inquiry Application User Log** – As explained in section 3 of the Blueprint, the JUSTIS POC allows users to access criminal justice data through an inquiry application. This functionality provides views into various agency criminal justice data stores in a common interface. Important to the management of any criminal justice information system is a verification and audit of who views the criminal justice data. Attached in Appendix C is an example of the current functionality developed in the JUSTIS POC to maintain the criminal justice data "audit trail." The reports lists the users id, name, and the criminal justice information viewed.

7. Glossary

10Base-T – One of several adaptations of the Ethernet (IEEE 802.3) standard for Local Area Networks (LANs). The 10Base-T standard (also called Twisted Pair Ethernet) uses a twisted-pair cable with maximum lengths of 100 meters.

100Base-T – A relatively new networking standard that supports data transfer rates up to 100 Mbps. 100BASE-T (IEEE 802.3u) is based on the older Ethernet standard. Because it is 10 times faster than Ethernet, it is often referred to as Fast Ethernet.

Access Control List (ACL) – A list of access control entries (ACEs), which contain information about a trustee, such as a user, group of users, or program.

ActiveX – A loosely defined set of technologies developed by Microsoft. An outgrowth of two other Microsoft technologies called OLE (Object Linking and Embedding) and COM (Component Object Model).

API – See "Application Programming Interface".

Applet – A program designed to be executed from within another application. Unlike an application, applets cannot be executed directly from the operating system.

Application Programming Interface (API) – a set of routines, protocols, and tools for building software applications.

Asynchronous Transfer Mode (ATM) – A network technology based on transferring data in cells or packets of a fixed size.

ATM – See "Asynchronous Transfer Mode".

Backbone – Network technology used to tie together multiple networks on an enterprise network.

Blue Pages – X.500 service that provides subject-matter listings of organizational programs and activities related to the organization such as the government blue pages.

Certificate – See Digital Certificate.

Certificate Authority – A Certificate Authority (CA) issues, verifies, and revokes certificates. The Certificate Authority's digital signature attests to the binding of the individual's identity and his public key.

Certificate Revocation List – A certificate revocation list is a list of digital certificates revoked before their scheduled expiration date.

CGI – See "Common Gateway Interface".

Clear Text – Information transmitted over a network in its original, unencrypted state.

Common Gateway Interface (CGI) – A specification for transferring information between a World Wide Web server and a CGI program. A CGI program is any program designed to accept and return data that

conforms to the CGI specification. The program could be written in any programming language, including C, Perl, or Visual Basic.

Digital Certificate – A digital certificate is a non-forgeable, tamper-proof electronic document that attests to the binding of an individual's identity with his or her public key. The information contained in the certificate is verified and sealed with the digital signature of a trusted third party, known as a Certificate Authority (CA). The CA will include in the certificate a range of dates within which it is valid.

Digital Signature – A digital signature is a portion of a message encrypted with a user's private key. The recipient knows that this message and its digital signature could have come only from the owner of the private key corresponding to the public key used to decrypt. Digital signatures not only verify the identity of the signer of messages, but also ensure that the messages have not been changed since their signing.

DHCP – See "Dynamic Host Configuration Protocol.

Dynamic Host Configuration Protocol (DHCP) – A protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network.

EC/EDI – Electronic Commerce (EC) applications such as Electronic Data Interchange (EDI) for commerce between business partners (e.g., banks, suppliers, manufacturers).

Encryption/Decryption – Encryption is the scrambling of a message into an unreadable form. Decryption is the reverse: an encrypted message is made readable. A key pair controls both encryption and decryption. If either key encrypts a message or file, only the other key in that pair can decrypt it. For example, if someone encrypts a message or file with an individual's public key, only that individuals private key can decrypt it. This assures message confidentiality. A manageable way to deploy encryption in a large environment is with the use of public key cryptography.

Ethernet – A local-area network (LAN) protocol that uses a bus topology and supports data transfer rates of 10 Mbps.

Extensible Markup Language (XML) – This new standard being developed by W3C is a simplified but strict subset of SGML that has features of validation, structure, and extensibility. XML is a standardized text format designed specifically for transmitting structured data to web applications.

FDDI – See "Fiber Distributed Data Interface".

Fiber Distributed Data Interface (FDDI) – A set of protocols for sending digital data over fiber optic cable. Generally used for WAN backbone. Supports data rates of up to 100 Mbps.

File Transfer Protocol (FTP) – A mechanism for transferring files between host computers over TCP/IP. FTP includes host-independent sub-commands for connecting and logging on to remote hosts; uploading and downloading files; listing directory contents; and changing the current working directory.

Firewall – A hardware/software device that restricts access between more than one network. A firewall is generally configured to block all externally initiated access, and to run any permitted internally initiated access via 'proxy' agents so that the internal computing device is never communicating directly with an external computing device.

Frame Relay – A packet-switching protocol for connecting devices on a Wide Area Network. Frame Relay networks support data transfer rates at T-1 (1.544 Mbps) and T-3 (45 Mbps) speeds

FTP – See "File Transfer Protocol".

Green Pages – X.500 service that provides browsing and querying of electronic information in documents and catalogs, such as documents statistics, photographs, multimedia records, and publications.

HTML – See "Hypertext Markup Language".

HTTP – See "Hypertext Transport Protocol".

Hypertext Markup Language (HTML) – The document encoding standard used for web pages. HTML supports embedded graphics, programs, and links to other objects such as web sites, documents, points within documents, images, and files that will automatically launch other desktop applications.

Hypertext Transport Protocol (HTTP) – The underlying protocol used by the World Wide Web. HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands.

IETF – See "Internet Engineering Task Force".

IMAP – See "Internet Messaging Access Protocol".

International Organization for Standardization (ISO) – ISO is an international organization composed of national standards bodies from over 75 countries, including ANSI (American National Standards Institute).

Internet Engineering Task Force (IETF) – The main standards organization for the Internet.

IPsec – A security protocol in the network layer being developed to provide cryptographic security services that will flexibly support combinations of authentication, integrity, access control, and confidentiality.

Internet Messaging Access Protocol (IMAP) – A protocol for retrieving email messages.

Internet Service Provider (ISP) – An organization that provides a connection to the Internet.

Intranet – A network based on TCP/IP (Internet) protocols, but belonging to an organization and accessible only by the organization's members, employees, or other authorized users.

Inter-network Packet Exchange (IPX) – A networking protocol used by the Novell NetWare operating systems. IPX is a datagram protocol used for connectionless communications.

International Telecommunications Union (ITU) – An intergovernmental organization established by the United Nations to develop international standards governing telecommunications.

IPX – See "Inter-network Packet Exchange".

ISO – See "International Organization for Standardization".

ISP – See "Internet Service Provider".

ITU – See “International Telecommunications Union”.

Java– A high-level programming language designed to be platform-independent. Java programs can be downloaded to a client as part of an HTML document and executed on that client.

kbps – Kilobits per second. Speed of data transmission in multiples of 1,024 bits (~128 characters) per second.

LAN – See “Local Area Network”.

Legacy system – Generally used to refer to working applications and platforms that do not employ consensus state-of-the-art technology.

Local Area Network (LAN) – A computer network that spans a relatively small area. A LAN generally serves a single building or floor of a building.

Mailhost – A server that routes incoming as well as outgoing email. Mail software (e.g., cc:Mail, MS Exchange) packages can store messages to be accessed by users or route mail to other mailhosts.

Management Information Base (MIB) – A database of objects that can be monitored by a network management system. Both SNMP and RMON use standardized MIB formats that allows any SNMP and RMON tools to monitor any device defined by a MIB.

Mbps – Megabits per second. Speed of data transmission in multiples of 1,048,576 bits (~131,072 characters) per second.

Meta-data or Meta-information – Data about data. Meta-data describes how and when and by whom a particular set of data was collected, and how the data is formatted.

Meta tag – An HTML tag that refers to meta-information, rather than to document text.

MIB – See “Management Information Base”.

Network News Transfer Protocol (NNTP) – Industry-standard method used by News group servers to receive downloads from an ISP; store the data for a predetermined amount of time, and distribute it to users upon request. The data consists of bulletin-board articles contributed by the Internet community.

NNTP – See “Network News Transfer Protocol”.

OLAP – See “On-line analytical processing”.

On-line analytical processing (OLAP) – A category of software tools that provides analysis of data stored in a database. OLAP tools enable users to analyze different dimensions of multidimensional data.

PDF – See “Portable Document Format”.

Portable Document Format (PDF) – A file format developed by Adobe Systems. Enables viewing of documents on screen as they would be printed.

Point-to-point protocol (PPP) – A protocol that allows a computer to access an Intranet or the Internet via a voice-grade telecommunications line and a modem.

POP3 – See “Post Office Protocol”.

Post Office Protocol (POP3) – A protocol used to retrieve email from a mail server.

PPP – See “Point-to-point Protocol”.

Private key – see Public key cryptography.

Public key – see Public key cryptography.

Public key cryptography – In a system that uses public key cryptography, each user is assigned two unique mathematically-related keys: a public key and a private key. The public key is published; the private key is kept secret, accessible only to the owner. Each key can read messages encrypted with the other key.

Push technology – Enables Internet based service delivery initiated by the information provider, rather than by the information requester.

RAS – See “Remote Access Server”.

RDBMS – See “Relational Database Management System”.

Relational Database Management System (RDBMS) – A collection of programs that enables you to store, modify, and extract information from a database.

Remote Access Server (RAS) – A computer or device that provides network access to users not directly connected to that network. Users generally access a RAS via dial-in modem or ISDN adapter.

Remote Monitoring (RMON) – A network management protocol that allows network information to be gathered at a single workstation. Whereas SNMP gathers network data from a single type of Management Information Base (MIB), RMON 1 defines nine additional MIBs that provide a much richer set of data about network usage.

RMON – See “Remote Monitoring”.

Router – A router is a hardware device that directs data flow between networks. The router’s software determines the best path to the destination computer from the client computer.

S/MIME – See “Secure Multipurpose Internet Mail Extension”.

Secure Multipurpose Internet Mail Extension (S/MIME) – A new version of the MIME protocol that supports encryption of messages. S/MIME is based on RSA's public-key encryption technology.

Search Engine – Software that reads documents and builds indices to collections of documents. This allows the user to search the index for key information, as well as document text.

Serial-line Internet protocol (SLIP) – A protocol that allows a computer to access an Intranet or the Internet via a voice-grade telecommunications line and a modem. SLIP is gradually being replaced by PPP.

SGML – See “Standard Generalized Markup Language”.

SLIP – See "Serial-line Internet protocol".

SNA – See "Systems Network Architecture".

SMTP – See "Simple Mail Transport Protocol".

SNMP – See "Simple Network Management Protocol".

Systems Network Architecture (SNA) – A set of network protocols developed by IBM to inter-connect mainframe computers.

Simple Network Management Protocol (SNMP) – A set of protocols for managing complex networks. SNMP works by sending messages, called protocol data units, to different parts of a network. SNMP-compliant devices, called agents, store data about themselves in Management Information Bases (MIBs) and return this data to the SNMP requesters.

Simple Mail Transport Protocol (SMTP) – A protocol for sending email messages between mail servers. SMTP is also used to send messages from a mail client to a mail server.

Standard Generalized Markup Language (SGML) – a system for organizing and tagging elements of a document.

T1 – A dedicated telecommunications connection supporting data rates of 1.544Mbits per second. A T-1 line actually consists of 24 individual channels, each of which supports 64Kbits per second.

T3 – A dedicated telecommunications connection supporting data rates of about 45Mbits per second. A T-3 line actually consists of 672 individual channels, each of which supports 64Kbits per second.

TCP/IP – See "Transmission Control Protocol over Internet Protocol".

Token Ring – A network that connects computers serially, (computer-to-computer) to form a loop, rather than via a hub, such as Ethernet.

Transaction Process Monitor (TP Monitor) – TP Monitor ensures that a transaction processes to completion and ensures that proper actions are taken if it fails to complete successfully.

Transmission Control Protocol over Internet Protocol (TCP/IP) – The suite of communications protocols used to connect hosts on the Internet. TCP/IP uses several protocols, the two main ones being TCP and IP.

Uniform Resource Locator (URL) – The standard naming convention used to identify a presence on the world wide web. This location can be a server (www.location.com); a directory on a server (www.location.com/ directory); a file on a server (www.location.com/directory/page.html); or a point on a file (www.location.com/page.html#refpoint). The location is preceded by the protocol used to access the location—e.g., http:// (for html documents) or ftp:// (for file transfers).

URL – See "Uniform Resource Locator".

Virtual Private Network (VPN) – A network that is constructed by using public wires to connect nodes. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted.

W3C – See "World Wide Web Consortium".

WAN – See "Wide Area Network".

Web – See "World Wide Web". When capitalized, "Web" typically refers to the World Wide Web on the Internet; lower-case "web" usually refers to the technology, regardless of whether it is deployed on the Internet or on a private Intranet.

Web Browser – A software application used to access information on a web-based network. A browser presents HTML-formatted documents, and it generally supports other protocols such as FTP.

Web Site – A single Web/Internet or private web/Intranet location (generally a web server or a directory on a web server).

White Pages – Basic "lookup" service for X.500 directories that presents personnel specific information such as telephone numbers, office locations, physical mailing addresses, and other personal and organizational attributes.

Wide Area Network (WAN) – A computer network that spans a relatively large geographical area. Typically, WAN consists of two or more local-area networks (LANs).

World Wide Web (WWW) – A system of Internet servers that support specially formatted documents. The documents are formatted in a language called HTML that supports links to other documents, as well as graphics, audio, and video files.

World Wide Web Consortium (W3C) – Organization of representatives from companies around the world that develops open standards used by the world wide web, such as HTML.

X.500 – An ISO and ITU standard that defines how global directories should be structured. X.500 directories are hierarchical with different levels for each category of information, such as country, state, and city. X.500 supports X.400 systems.

X.509 – X.509, or ISO/IEO 9594-8, is widely recognized as the leading network and communications security architecture standard specification. Any application or device can use the standardized security and authentication services of X.509. The authentication-framework specification within X.509 addresses the handling of public keys via certificates and certificate revocation lists.

XML – See "Extensible Markup Language".

Yellow Pages – X.500 service that presents detailed information on products and services to facilitate organizational procurement activities.